

(43) Date of publication of application: 10 . 12 . 99

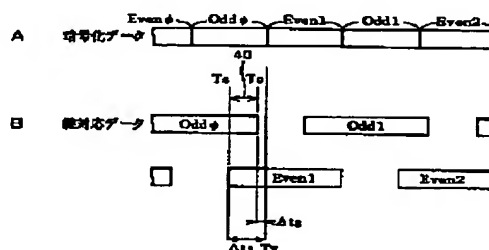
(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

(72) Inventor: **SUGIMOTO YOSHIYUKI**

COPYRIGHT: (C)1999,JPO

**PROBLEM TO BE SOLVED:** To shorten the time for acquiring images or voices by shortening the time to be occupied for sending out a cryptographic key by sending out key correspondent data so as to correspond to not only a key at that time but also a key to be next used within a prescribed overlap period before the time of changing a key used in enciphered data.

**SOLUTION:** In the Fig. B, sections Odd0, Even1, Odd1 and Even2 are respectively periods for sending out the key correspondent data of cryptographic keys Odd0, Even1, Odd1 and Even2. Preceding to a time  $T_x$  to change the cryptographic key used in the enciphered data by  $\Delta t_1$  (Ts), the next key correspondent data are sent out. This is for receiving data without interrupting them while considering the time for restoring the cryptographic key from the key correspondent data on the reception side. Besides, the key correspondent data of the cryptographic key just used or enciphering data at present as well as continuously sent out even after the transmission of the next key correspondent data is



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-340966

(43) 公開日 平成11年(1999)12月10日

(51) Int.Cl.<sup>5</sup>

識別記号

F I

H 0 4 L 9/14

H 0 4 L 9/00

6 4 1

H 0 4 K 1/04

H 0 4 K 1/04

H 0 4 N 7/167

H 0 4 N 7/167

Z

審査請求 未請求 請求項の数19 O L (全 30 頁)

(21) 出願番号

特願平10-145372

(22) 出願日

平成10年(1998)5月27日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 杉本 圭志

愛知県名古屋市中区栄2丁目6番1号 白

川ビル別館5階 株式会社松下電器情報シ

ステム名古屋研究所内

(74) 代理人 弁理士 古谷 栄男 (外3名)

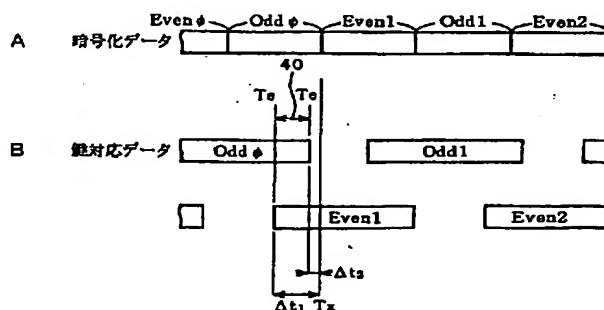
(54) 【発明の名称】 鍵を用いた通信システムおよび方法

(57) 【要約】

【課題】 暗号鍵送出のための占有時間が短く、かつ、受信開始時に、画像および音声を得られるまでの時間が短い通信システム、並びにかかるシステムにおいて所望の結果を得るための通信パラメータの設定を容易にすることを目的とする。

【解決手段】 暗号化データと鍵対応データは、図2に示すようなタイミングにて送出される。図2Bに示すように、暗号化データにおいて用いた暗号鍵が変わる時点 $T_x$ より $\Delta t_1$ だけ早く( $T_s$ 参照)、次の鍵対応データを送出している。これは、受信側において、鍵対応データから暗号鍵を復元するための時間を考慮して、データが途切れることなく受信できるようにするためである。上記のように、一部において重複期間40を設けることにより、鍵対応データによる通信路の占有をできるだけ小さくしつつ、特に処理開始時における受信側での復元データの連続的な受信を確保するようにしている。

暗号化データと鍵対応データの送出タイミング



## 【特許請求の範囲】

【請求項 1】 所定時間ごとに鍵を変えて送出すべきデータを暗号化して送出する (a) 送信装置と (b) 受信装置とを備えた鍵を用いた通信システムであって：前記送信装置は、

(a1) 順次異なる鍵を出力する鍵出力手段と、  
 (a2) 鍵出力手段から取得した鍵に基づいて、送出すべきデータを暗号化して暗号化データを生成する暗号化手段と、  
 (a3) 鍵出力手段からの鍵を、対応する鍵対応データに変換する鍵対応データ生成手段と、  
 (a4) 順次異なる鍵によって暗号化された暗号化データと、当該暗号化に用いた鍵に対応する鍵対応データとを送出する送出手段であって、暗号化データに用いた鍵が変わる時点より前の所定重複期間内においては、当該時点での鍵だけでなく次に使用する鍵にも対応するように鍵対応データを送出する送出手段と、  
 を備えており、  
 前記受信装置は、

(b1) 送信されてくる暗号化データと鍵対応データとを受け取る受取手段と  
 (b2) 受取手段によって受け取った鍵対応データに基づいて、鍵を生成する鍵取得手段と、  
 (b3) 受取手段によって受け取った暗号化データを、鍵取得手段によって取得した鍵に基づいて復号化する復号化手段であって、暗号化データに対する処理の開始時点が前記重複期間外である場合は、鍵が取得できた後に復号化したデータの出力を開始するとともに、暗号化データに対する処理の開始時点が前記重複期間内である場合は、少なくとも次に使用する鍵が取得できた後に復号化したデータの出力を開始する復号化手段と、  
 を備えていることを特徴とする通信システム。

【請求項 2】 所定時間ごとに鍵を変えて送出すべきデータを暗号化して送出し、受信側において暗号化データを復号化する通信方法であって、  
 順次異なる鍵に基づいて、送出すべきデータを暗号化して暗号化データを生成し、

順次異なる鍵によって暗号化された暗号化データと、当該暗号化に用いた鍵に対応する鍵対応データとを送出するに際して、

暗号化データに用いた鍵が変わる時点より前の所定重複期間内において、当該時点での鍵だけでなく次に使用する鍵にも対応するように鍵対応データを送出するとともに、

送出されてきた暗号化データと鍵対応データとを受け取り、

受け取った鍵対応データに基づいて鍵を生成し、

受け取った暗号化データを鍵に基づいて復号化するに際し、暗号化データに対する処理の開始時点が前記重複期間外である場合は、鍵が取得できた後に復号化したデー

タの出力を開始するとともに、暗号化データに対する処理の開始時点が前記重複期間内である場合は、少なくとも次に使用する鍵が取得できた後に復号化したデータの出力を開始するものであることを特徴とする通信方法。

【請求項 3】 所定時間ごとに鍵を変えて送出すべきデータを暗号化して送出する送信装置であって、  
 順次異なる鍵を出力する鍵出力手段と、  
 鍵出力手段から取得した鍵に基づいて、送出すべきデータを暗号化して暗号化データを生成する暗号化手段と、  
 鍵出力手段からの鍵を、対応する鍵対応データに変換する鍵対応データ生成手段と、  
 順次異なる鍵によって暗号化された暗号化データと、当該暗号化に用いた鍵に対応する鍵対応データとを送出する送出手段であって、暗号化データに用いた鍵が変わる時点より前の所定重複期間内においては、当該時点での鍵だけでなく次に使用する鍵にも対応するように鍵対応データを送出する送出手段と、  
 を備えた送信装置。

【請求項 4】 所定時間ごとに鍵を変えて送出すべきデータを暗号化して通信する通信方法であって、  
 順次異なる鍵に基づいて、送出すべきデータを暗号化して暗号化データを生成し、  
 順次異なる鍵によって暗号化された暗号化データと、当該暗号化に用いた鍵に対応する鍵対応データとを送出するに際して、  
 暗号化データに用いた鍵が変わる時点より前の所定重複期間内においては、当該時点での鍵だけでなく次に使用する鍵にも対応するように鍵対応データを送出することを特徴とする通信方法。

【請求項 5】 請求項 4 の通信方法において、  
 前記重複期間内においては、当該時点での鍵に対応する鍵対応データと、次に使用する鍵に対応する鍵対応データとの 2 つの鍵対応データを送出することを特徴とするもの。

【請求項 6】 請求項 4 の通信方法において、  
 前記重複期間内においては、当該時点での鍵と次に使用する鍵とに対応する 1 つの鍵対応データを送出することを特徴とするもの。

【請求項 7】 請求項 5 または 6 の通信方法において、  
 前記重複期間の開始時点  $T_s$  は、下式によって示されるものであることを特徴とするもの：

$$T_s = T_x - R_{\max} - \alpha$$

ここで、 $T_x$  は暗号化データにおいて鍵が変わる時点、 $R_{\max}$  は受信側において、前記重複期間外に受けた鍵対応データから鍵を取得するに必要な時間と、前記重複期間内に受けた鍵対応データから次の鍵を取得するに必要な時間とを合計した時間のうち想定した最も大きな時間、 $\alpha$  は余裕時間である。

【請求項 8】 請求項 5、6 または 7 の通信方法において、

前記重複期間の終了時点 $T_e$ は、下式によって示されるものであることを特徴とするもの：

$$T_e = T_x - R_{min} + \beta$$

ここで、 $T_x$ は暗号化データにおいて鍵が変わる時点、 $R_{min}$ は受信側において、前記重複期間外に受けた鍵対応データから鍵を取得するに必要な時間と、前記重複期間内に受けた鍵対応データから次の鍵を取得するに必要な時間とを合計した時間のうち想定した最も小さな時間、 $\beta$ は余裕時間である。

【請求項 9】所定時間ごとに鍵を変えて暗号化された暗号化データと当該鍵に対応する鍵対応データとを受けて、暗号化データを復号化する受信装置であって、受け取った鍵対応データに基づいて、鍵を生成する鍵取得手段と、  
受取手段によって受け取った暗号化データを、鍵取得手段によって取得した鍵に基づいて復号化する復号化手段であって、暗号化データに対する処理の開始時点において、1つの鍵に対応する鍵対応データを受けている場合には、鍵が取得できた後に復号化したデータの出力を開始するとともに、暗号化データに対する処理の開始時点において、2つの鍵に対応する鍵対応データを受けている場合には、少なくとも次の鍵が取得できた後に復号化したデータの出力を開始する復号化手段と、  
を備えた受信装置。

【請求項 10】請求項 9 の受信装置において、  
前記 2 つの鍵に対応する鍵対応データは、現在の鍵に対応する鍵対応データと次の鍵に対応する鍵対応データとの 2 つの鍵対応データとして与えられ、前記 1 つの鍵に対応する鍵対応データは、現在の鍵に対応する 1 つの鍵対応データとして与えられており、  
前記復号化手段は、暗号化データに対する処理の開始時点において、現在の鍵に対応する 1 つの鍵対応データを受けている場合には、当該鍵が取得できた後に復号化したデータの出力を開始し、暗号化データに対する処理の開始時点において、現在の鍵および次の鍵に対応する 2 つの鍵対応データを受けている場合には、少なくとも次の鍵が取得できた後に復号化したデータの出力を開始するものであることを特徴とする受信装置。

【請求項 11】請求項 10 の受信装置において、  
前記復号化手段は、暗号化データに対する処理の開始時点において、現在の鍵および次の鍵に対応する 2 つの鍵対応データを受けている場合には、現在の鍵を先に取得した際には、2 つの鍵対応データが送信される期間の終了時点から鍵が変更される時点までの時間よりも、鍵対応データから次の鍵を取得する時間の方が短い場合には、次の鍵の取得を待たずに現在の鍵を取得した時点で、復号化したデータの出力を開始することを特徴とする受信装置。

【請求項 12】請求項 9 の受信装置において、  
前記 2 つの鍵に対応する鍵対応データは、現在の鍵およ

び次の鍵に対応する 1 つの鍵対応データとして与えられ、前記 1 つの鍵に対応する鍵対応データは、現在の鍵が 1 つの鍵対応データとして与えられており、

前記復号化手段は、暗号化データに対する処理の開始時点において、現在の鍵に対応する 1 つの鍵対応データを受けている場合には、当該鍵が取得できた後に復号化したデータの出力を開始し、暗号化データに対する処理の開始時点において、現在の鍵および次の鍵に対応する 1 つの鍵対応データを受けている場合には、少なくとも次の鍵が取得できた後に復号化したデータの出力を開始するものであることを特徴とする受信装置。

【請求項 13】請求項 12 の受信装置において、  
前記復号化手段は、現在の鍵および次の鍵が含まれている 1 つの鍵対応データを受けた場合には、当該 2 つの鍵のうち、まだ復元していない次の鍵のみを復元するものであることを特徴とする受信装置。

【請求項 14】所定時間ごとに鍵を変えて暗号化された暗号化データと当該鍵に対応する鍵対応データとを受けて、暗号化データを復号化する受信装置であって、暗号化データを鍵に基づいて復号化して出力する復号化出力部と、  
復号化出力部の動作を制御する処理部と、  
処理部の処理内容を定めたプログラムを記録している記録部と、  
を備え、

前記プログラムは、処理部に接続された鍵復元部に鍵対応データを与えて鍵を復元させ、  
復号化出力部において、受け取った暗号化データを、前記生成された鍵に基づいて復号化させるに際して、暗号化データに対する処理の開始時点において、1つの鍵に対応する鍵対応データを受けている場合には、鍵が取得できた後に復号化したデータの出力を開始するとともに、暗号化データに対する処理の開始時点において、2つの鍵に対応する鍵対応データを受けている場合には、少なくとも次の鍵が取得できた後に復号化したデータの出力を開始するよう制御するものであること、  
を特徴とする受信装置。

【請求項 15】所定時間ごとに鍵を変えて暗号化された暗号化データを復号化する復号化装置であって、暗号化データに対する処理の開始時点において、1つの鍵に対応する鍵対応データを受けている場合には、鍵が取得できた後に復号化したデータの出力を開始するとともに、暗号化データに対する処理の開始時点において、2つの鍵に対応する鍵対応データを受けている場合には、少なくとも次の鍵が取得できた後に復号化したデータの出力を開始するように構成されていることを特徴とする復号化装置。

【請求項 16】所定時間ごとに鍵を変えて暗号化された暗号化データを復号化する処理を制御するためのプログラムを記録した記録媒体であって、

当該プログラムは、受け取った鍵対応データに基づいて鍵を生成させ、

受け取った暗号化データを、前記生成された鍵に基づいて復号化させるに際して、暗号化データに対する処理の開始時点において、1つの鍵に対応する鍵対応データを受けている場合には、鍵が取得できた後に復号化したデータの出力を開始するとともに、暗号化データに対する処理の開始時点において、2つの鍵に対応する鍵対応データを受けている場合には、少なくとも次の鍵が取得できた後に復号化したデータの出力を開始するよう制御するものであること、

を特徴とするプログラムを記録した記録媒体。

【請求項17】 鍵対応データを受けて鍵を再生する鍵再生装置であって、

受け取った鍵対応データに対応する鍵の個数を検出する個数検出手段と、

当該個数検出手段によって検出された個数の鍵を、鍵対応データから再生する鍵再生手段と、

を備えたことを特徴とする鍵再生装置。

【請求項18】 所定時間ごとに鍵を変えて暗号化された暗号化データと当該鍵に対応する鍵対応データとを受けて、暗号化データを復号化する通信方法であって、暗号化データと鍵対応データとを受け取り、受け取った鍵対応データに基づいて鍵を生成し、受け取った暗号化データを鍵に基づいて復号化するに際して、暗号化データに対する処理の開始時点において2つの鍵に対応する鍵対応データを受けている場合には、取得した現在の鍵に基づいて暗号化データを復号化するとともに取得した次の鍵を保持し、暗号化データに対する処理の開始時点において1つの鍵に対応する鍵対応データを受けている場合には、取得した鍵に基づいて暗号化データを復号化するようにしたことを特徴とする通信方法。

【請求項19】 請求項18の通信方法において、暗号化データに対する処理の開始時点において、1つの鍵に対応する鍵対応データを受けている場合には、当該鍵が取得できた後に復号化したデータの出力を開始するとともに、暗号化データに対する処理の開始時点において、2つの鍵に対応する鍵対応データを受けている場合には、少なくとも次に使用する鍵が取得できた後に復号化したデータの出力を開始するようにしたことを特徴とする通信方法。

【発明の詳細な説明】

【0001】

【発明の技術分野】 この発明は暗号鍵による暗号化通信に関するものであり、特にその暗号鍵の伝送に関するものである。

【0002】

【従来の技術】 図37に、従来の衛星デジタル放送受信機の構成をブロック図にて示す。衛星デジタル放送にお

いては、画像データ、音声データ、制御データなどが、時分割のバケットとして送られてくる。また、このバケットは、暗号鍵によって暗号化されている。

【0003】 チューナ部2は、制御部4の制御に応じ、衛星から送信されてくる電波から、所望のトランスポートストリーム（周波数、偏波面などによって決定される伝送路）のバケット（TSバケットと呼ぶ）を選択的に受信する。出力されたTSバケットには、複数のチャンネルの画像データ、音声データ、制御データが時分割で含まれている。

【0004】 デ・スクランブル部6は、制御部4の制御に従って、暗号鍵に基づきTSバケットの暗号を解除する。さらに、デコーダ部8は、制御部4の制御に従って、TSバケットから、所望のチャンネルの画像データ、音声データ、制御データを選択的に取得する。NTSCエンコーダ10は、デコーダ部8によって得られた画像データ、音声データに基づいて、NTSCコンポジット信号を生成する。

【0005】 ところで、放送局側から送られてくるTSバケットは、守秘性を高くするために、リアルタイムに暗号鍵を変えて伝送されてくるようになっている。その伝送状態を、図38に示す。たとえば、図中のTSバケットにおいて、Odd0と表示された期間では、複数のTSバケットがOdd0の暗号鍵によって暗号化されている。同様に、Even1、Odd1、Even2の期間では、複数のTSバケットが、それぞれ、暗号鍵Even1、Odd1、Even2によって暗号化されている。

【0006】 TSバケットの一部として、これら暗号鍵Odd0、Even1、Odd1、Even2自体を暗号化したECMデータも併せて送信されてくる。このECMデータは何度も繰り返し送信される。図38は、ECMデータが繰り返し送信される期間を示している。

【0007】 図38から明らかなように、TSバケットにおいて現在用いられている暗号鍵のECMデータだけでなく、次に用いられる暗号鍵のECMデータも同時に送信されている。たとえば、図のT1のタイミングで受信を開始すると、デ・スクランブル部6は、受信したECMデータに基づいて、暗号鍵Odd0、Even1を復元する。この暗号鍵の復元にt1要するとすれば、T1+t1のタイミングから画像および音声出力されることとなる。その後は、予め、次の暗号鍵が復元されて得られているので、とぎれることなく画像および音声出力される。

【0008】 上記のように、常に、現在の暗号鍵と次の暗号鍵を取得することができるので、どのようなタイミングでチャンネルの切替があっても、暗号鍵の復元時間t1だけ待てば、画像および音声を得られる。

【0009】 また、図39に示すようにして、暗号鍵のECMデータを伝送する方式もある。この方式では、TSバケットに用いている暗号鍵のECMデータを、所定

時間 $\Delta t$ だけ早く送信している。ECMデータから暗号鍵を復元するために要する時間よりも、この $\Delta t$ を大きくしておけば、とぎれることなく画像および音声を出力することができる。ECMデータから暗号鍵を復元するために要する時間は、受信機によって異なる。したがって、各種受信機においてECMデータから暗号鍵を復元するために要する時間のうち、最大の時間 $t_{\max}$ よりも $\Delta t$ が大きくなるように設定すれば、全ての受信機において、とぎれることなく画像および音声を得ることができる。

#### 【0010】

【発明が解決しようとする課題】上記のような従来の通信方式には、次のような問題点があった。

【0011】図38に示すような方式においては、2つの暗号鍵を1つのECMデータとして送るようにしているので、ECMデータが長くなって、ECMデータの送出のための時間が長くなるという問題点があった。また、ECMデータから暗号鍵を復元するための時間が長くなるという問題もあった。

【0012】これに対し、図39に示すような方式においては、1つの暗号鍵のみをECMデータとして送るようにしているので、ECMデータ送出のための時間が短く、暗号鍵復元に要する時間も短いという利点がある。

【0013】しかしながら、暗号鍵復元に最も時間を要する受信機の復元時間 $t_{\max}$ を考慮して $\Delta t$ を設定しているので、チャンネル切替時に、画像および音声が出力されるまでの時間がかかるという問題があった。図40に、この問題点を説明するため、図38の方式と図39の方式とを比較して示す。ここで、タイミングT2において、チャンネルが切り換えられて受信が開始されたとする。受信機が暗号鍵Odd0の復元に要する時間を $t_1$ とすれば、図38の方式の場合には、 $T2 + t_1$ のタイミングから、画像および音声を得られることとなる。これに対し、図39の方式の場合には、タイミングT2においては、もはや暗号鍵Odd0のECMデータが送られてきていないので、タイミングT3まで画像および音声を得られないことになってしまう。このように、図39の方式では、ECMデータ送出のための時間が短く、暗号鍵復元に要する時間も短いという利点があるものの、チャンネル切り替え時などの受信開始時に、画像および音声を得られるまでの時間が長くなってしまいう問題があった。

【0014】さらに、図39の方式では、 $\Delta t$ を、暗号鍵復元に最も時間を要する受信機の復元時間 $t_{\max}$ と等しくしておいても、チャンネル切換時には、一旦表示された画像等が途切れるという現象が生じている。かかる現象については、経験上 $\Delta t$ を大きくとることによって解決できることが分かっている。しかしながら、前述のように、 $\Delta t$ をあまり大きくすると、復元処理の速い受信機においても、チャンネル切換時に映像等が得られるまで

の時間が長くなるという問題を生じる。そこで、従来、試行錯誤によって適切な $\Delta t$ の長さを決定しており、極めて煩雑であった。つまり、適切な結果を得るための通信パラメータの設定が困難であった。

【0015】この発明は、上記のような問題点を解決して、暗号鍵送出のための占有時間が短く、かつ、受信開始時に、画像および音声を得られるまでの時間が短い通信システムおよび方法等を提供すること、並びにかかるシステムおよび方法において所望の結果を得るための通信パラメータの設定を容易にすることを目的とする。

#### 【0016】

【課題を解決するための手段および発明の効果】この発明に係る通信システムおよび方法は、所定時間ごとに鍵を変えて送出すべきデータを暗号化して送出し、受信側において暗号化データを復号化する通信システムおよび方法であって、送信側においては、順次異なる鍵に基づいて、送出すべきデータを暗号化して暗号化データを生成し、順次異なる鍵によって暗号化された暗号化データと、当該暗号化に用いた鍵に対応する鍵対応データとを送出するに際して、暗号化データに用いた鍵が変わる時点より前の所定重複期間内において、当該時点での鍵だけでなく次に使用する鍵にも対応するように鍵対応データを送出するとともに、受信側においては、送出されてきた暗号化データと鍵対応データとを受け取り、受け取った鍵対応データに基づいて鍵を生成し、受け取った暗号化データを鍵に基づいて復号化するに際し、暗号化データに対する処理の開始時点が前記重複期間以外の期間である場合は、鍵が取得できた後に復号化したデータの出力を開始するとともに、暗号化データに対する処理の開始時点が前記重複期間である場合は、少なくとも次の鍵が取得できた後に復号化したデータの出力を開始するものであることを特徴としている。

【0017】上記のように、暗号化データに用いた鍵が変わる時点より前の所定重複期間においてのみ、当該時点での鍵だけでなく次に使用する鍵にも対応するように鍵対応データを送出するようにしている。たとえば、重複期間において、当該時点での鍵に対応する鍵対応データと、次に使用する鍵に対応する鍵対応データとの2つの鍵対応データを送出するようにしたり、当該時点での鍵と次に使用する鍵とに対応する1つの鍵対応データを送出するようにしている。したがって、鍵対応データ送出のための占有時間を短くしつつ、受信開始時に、画像および音声を得られるまでの時間を短くすることができる。

【0018】この発明では、重複期間の開始時点 $T_s$ が、下式によって示されるものであることを特徴としている。

$$【0019】T_s = T_x - R_{\max} - \alpha$$

ここで、 $T_x$ は暗号化データにおいて鍵の変わる時点、 $R_{\max}$ は受信側において、重複期間外に受けた鍵対応データ

から鍵を取得するに必要な時間と、重複期間内に受けた鍵対応データから次の鍵を取得するに必要な時間とを合計した時間のうち想定した最も大きな時間、 $\alpha$ は余裕時間である。

【0020】上記のようにRmaxを定めて重複期間の開始時点Tsを定めることにより、重複期間の始まる直前に処理を開始した場合であっても、途切れることなく復号化されたデータを得ることができる。また、想定した受信装置のうち、鍵対応データから鍵を復元する処理の最も遅い受信装置によってRmaxを定めているので、想定される全ての受信機において、これを達成することができる。また、処理開始時に途切れることなく復号化されたデータを得るために、重複期間の開始時期をどのように設定すればよいのかが明確となってシステム設計が容易となる。

【0021】この発明では、重複期間の終了時点Teが、下式によって示されるものであることを特徴としている。

$$【0022】Te = Tx - Rmin + \beta$$

ここで、Rminは受信側において、重複期間外に受けた鍵対応データから鍵を取得するに必要な時間と、重複期間内に受けた次の鍵に対応する鍵対応データから鍵を取得するに必要な時間とを合計した時間のうち想定した最も小さな時間、 $\beta$ は余裕時間である。

【0023】現在使用する鍵が復元できた時点で、使用する鍵が次の鍵に変わっていた場合には、鍵の復元処理が無駄になる。そこで、想定した受信装置のうち、鍵対応データから鍵を復元する処理の最も速い受信装置に基づいて、重複期間の終了時点Teを、鍵の変化時点Txよりも前に終了させることにより、復元化されたデータの受信に支障を与えることなく重複期間を短くすることができる。

【0024】この発明では、受信側での暗号化データの処理開始時点において、2つの鍵に対応する鍵対応データを受けている場合には、少なくとも次の鍵が取得できた後に復号化したデータの出力を開始するようにしている。したがって、処理開始の際に、復元化されたデータを途切れることなく受信することができる。

【0025】この発明では、受信側での暗号化データの処理開始時点において、2つの鍵対応データを受けており、現在の鍵を先に取得した際には、2つの鍵対応データが送信される期間の終了時点から鍵が変更される時点までの時間よりも、鍵対応データから次の鍵を取得する時間の方が短い場合には、次の鍵の取得を待たずに現在の鍵を取得した時点で、復号化したデータの出力を開始することを特徴としている。したがって、処理の開始から復号化したデータの出力までの時間を、受信装置の処理速度に応じて短くすることができる。

【0026】この発明では、2つの鍵が含まれている鍵対応データを受けた場合には、当該2つの鍵のうち、ま

だ復元していない鍵のみを復元するものであることを特徴としている。したがって、鍵の復元処理時間を短くすることができる。

【0027】この発明において、「通信」とは、一斉放送、1対1通信等の形態を問わないものである。また、有線通信、無線通信を問わない。

【0028】「受信装置」とは、暗号化されたデータを受けて、復号化して出力する機能を有する装置をいう。たとえば、衛星放送テレビジョンの電波を受信して、コンポジット信号として出力するセット・トップ・ボックス(STB)や、STBの機能を内蔵したTVセットなどがこれに該当する。

【0029】「鍵出力手段」とは、暗号化のための鍵を自ら生成する手段だけでなく、他の手段から受け取った鍵を保持して出力する手段も含む概念である。

【0030】「復号化手段」とは、暗号化されたデータを受けて、これを鍵に基づいて復号化し、出力する手段をいう。実施形態においては、図12のデ・スクランブラ68、トランスポートデコーダ70およびCPU72(特に図17、図23、図32、図36に示す処理)が、これに対応する。

【0031】「2つの鍵に対応する鍵対応データを受け」とは、それぞれが1つの鍵に対応する鍵対応データを2つ受ける場合だけでなく、2つの鍵に対応する鍵対応データを1つ受ける場合をも含む概念である。実施形態では、前者は図10に対応し、後者は図31に対応する。

【0032】「暗号化データに対する処理の開始時点」とは、当該暗号化データを復号化するために必要な鍵対応データを受け取った時点を行い、実施形態においては、図18～図22等の時点X1がこれに該当する。

【0033】「送出すべきデータ」とは、暗号化して送信される対象となるデータであり、画像データ、音声データだけでなく、文書テキストデータ、プログラムデータ等であってもよい。

【0034】「プログラムを記録した記録媒体」とは、CPUによって実行可能なプログラムを記録した、ROM、RAM、ハードディスク、フレキシブルディスク、CD-ROM等の記録媒体をいう。また、プログラムは、CPUによって直接実行可能なものだけでなく、一旦インストールが必要なもの、圧縮されているもの、暗号化されているものも含まれる。

【0035】

【発明の実施の形態】1. システムの全体構成

(1) システムのブロック図

この発明の一実施形態による通信システムの全体構成を図1に示す。この通信システムは、送信装置20と受信装置22を備えている。また、送信装置20と受信装置30とは、地上波通信、衛星通信、有線通信、WAN、LAN等の通信路(図示せず)によって結合されてい



る。

【0036】送信装置20は、鍵出力手段22、暗号化手段24、鍵対応データ生成手段26、送出手段28を備えている。鍵出力手段22は、暗号化のための鍵を次々と生成する。暗号化手段24は、送出すべきデータを鍵出力手段22からの暗号鍵によって暗号化して、暗号化データを生成する。鍵対応データ生成手段26は、鍵出力手段22からの暗号鍵自体を暗号化して、鍵対応データを生成する。送出手段28は、暗号化データとその暗号化に用いられた暗号鍵の鍵対応データとを送出する。

【0037】受信装置30は、受取手段32、複合化手段34、鍵取得手段36を備えている。受取手段32は、送信装置20から送られてきた暗号化データおよび鍵対応データを受け取る。鍵取得手段36は、受け取った鍵対応データから暗号鍵を復元する。複合化手段34は、鍵取得手段36によって復元された暗号鍵に基づいて、暗号化データを復号化してデータを取得して出力する。

【0038】なお、図1においては、1つの送信装置に対して1つの受信装置を示している。しかしながら、この通信システムの適用分野によって、送信装置と受信装置の対応関係は異なったものとなる。たとえば、衛星放送システムに適用した場合には、1つの送信装置20に対して、多くの受信装置30が対応することとなる。また、受信装置30が多くの衛星放送システムに対応している場合、受信装置30の側から見れば、複数の送信装置20に対して、1つの受信装置30が対応することとなる。また、LANなどのネットワーク通信に適用した場合には、複数の送信装置20に対して、複数の受信装置30が対応することとなる。

#### 【0039】(2)通信方法の概要

図1に示す通信システムにおける暗号化データと鍵対応データの送出タイミングを、図2に示す。鍵出力手段22は、暗号鍵を順次出力する。ここでは、一連の暗号鍵をEven0, Odd0, Even1, Odd1, Even2...と表すこととする。Even0, Even1...を偶数鍵、Odd0, Odd1, Odd2...を奇数鍵という。暗号化手段24は、送出すべきデータに対し期間を区切って、これら一連の暗号鍵によって暗号化を行って暗号化データを生成する。この状態を図2Aに示す。

【0040】送出手段28は、暗号化データと鍵対応データを図2に示すようなタイミングにて送出する。なお、図2Bにおいて、Odd0, Even1, Odd1, Even2と示した部分は、それぞれ、暗号鍵Odd0, Even1, Odd1, Even2の鍵対応データを送出している期間であることを示している。また、各期間において、鍵対応データは、1回だけでなく複数回繰り返して同じものを送出するようにしている。これにより、鍵対応データの受信に失敗しても、再度、鍵対応データを受信して暗号鍵を得ることができ

る。

【0041】図2Bに示すように、暗号化データにおいて用いた暗号鍵が変わる時点Txより $\Delta t1$ だけ早く( $T_s$ 参照)、次の鍵対応データを送出している。

【0042】これは、受信側において、鍵対応データから暗号鍵を復元するための時間を考慮して、データが途切れることなく受信できるようにするためである。したがって、 $\Delta t1$ は、受信側の状況によって想定される暗号鍵復元時間のうち最悪の場合(最も時間がかかる場合)の時間を基準として、これと等しいかもしくは、わずかに大きいことが好ましい。複数の受信装置において最も復元の遅い装置の復元時間を基準としたり、1つの受信装置において処理負荷状況などによって変化する復元時間のうち最も遅いものを基準としたりすればよい。

【0043】また、暗号化データの暗号化に現在用いられている暗号鍵の鍵対応データは、次の鍵対応データが送出され始めてからも、引き続き送出されている。したがって、この期間40は、現在の鍵対応データと次の鍵対応データとが重複して送出されることとなる。この期間を重複期間と呼ぶ。現在の鍵対応データは、暗号鍵が変わる時点Txより $\Delta t2$ だけ早い時点Telにおいて、送出が停止される。

【0044】これは、受信側において、鍵対応データから暗号鍵を復元するための時間を考慮して、不要な鍵対応データを送出しないようにするためである。つまり、鍵対応データから暗号鍵が復元できた時点において、すでに使用されている暗号鍵が次のものになっている場合には、その鍵対応データを送る必要はない。むしろ、鍵対応データを送ることによって、伝送路の実質的な伝送容量を低下させることとなる。したがって、 $\Delta t2$ は、受信側の状況によって想定される暗号鍵復元時間のうち最良の場合(最も時間がかからない場合)の時間を基準として、これと等しいかもしくは、わずかに小さいことが好ましい。複数の受信装置において最も復元の速い装置の復元時間を基準としたり、1つの受信装置において処理負荷状況などによって変化する復元時間のうち最も速いものを基準としたりすればよい。

【0045】図2Bに示す重複期間40を設けることにより、受信側における受信処理開始時でのデータ出力までの時間を、受信装置の性能や状況に応じて短くすることができる。つまり、いずれの受信装置においても、あるいは受信装置の処理状況がどのような状態にあっても、ほぼ、暗号鍵の復元時間経過後にデータの出力を得ることができる。

#### 【0046】2. 衛星放送システムにおける第1の実施形態

次に、この発明による通信システムを衛星放送システムに適用した場合の実施形態について説明する。

##### 【0047】(1)送信装置の構成の説明

衛星放送においては、周波数や偏波方向などによって決



定される各トランスポンダのそれぞれに複数のチャンネルが設定される。各トランスポンダにおいては、時分割によって複数チャンネルのデータがパケット化されて送信されている。各トランスポンダによって伝送されるデータを、トランスポートストリームと呼ぶ。

【0048】図3に、トランスポートストリームを生成して送信するための送信装置の構成を示す。図においては、1組の画像データ、音声データのみを示しているが、多数の画像データ、音声データの組が与えられる。音声データ、画像データの組は、所定個数ごとに1つのトランスポートストリームにまとめられる。

【0049】画像データ42は、画像エンコーダ48によって圧縮されて多重化部54に与えられる。同様に、音声データ44は、音声エンコーダ50によって圧縮されて多重化部54に与えられる。なお、この実施形態では、MPEG2規格に基づいてデータの圧縮を行っている。

【0050】制御データ生成部46は、パケット化のための制御データを生成する。この制御データは、時分割された複数チャンネルの画像データ、音声データを正しく識別するためのために付される。多重化部52は、制御データ、圧縮された画像データ、音声データおよび後述するECMデータを時分割して固定長のパケットにし、トランスポートストリームとして出力する。この際、多重化部54は、誤り訂正の符号を付加する。この実施形態では、畳み込み符号化を内符号、短縮化リードソロモン符号を外符号とする接続符号によって、誤り訂正を行っている。

【0051】スクランブラ56は、出力されたパケットに対し、スクランブル鍵制御部60から与えられるスクランブル鍵を用いてスクランブルをかける。スクランブルのかけられたトランスポートストリームは、変調部58において変調され、放送衛星を介して視聴者に放送される。

【0052】なお、スクランブラ56において用いられたスクランブル鍵は、ECM生成部52において暗号化され、鍵対応データであるECM(Entitlement Control Message)データとされる。多重化部54は、このECMデータも含めてパケット化する。

【0053】この実施形態においては、エネルギー拡散方式を用いて、M系列により発生する疑似ランダム信号を加算することにより、スクランブルをかけるようにしている。なお、この他の暗号化方式によってスクランブルをかけるようにしても良い。

【0054】(2)トランスポートストリームの構造  
図3の送信装置によって生成されたトランスポートストリームの構造を説明する。この実施形態では、パケット化の制御データとして、MPEG2システムに規定されるPSI(Program Specific Information)を用いている。

【0055】図4を参照して、3つのチャンネルを時分割多重化したトランスポートストリームの構造を説明す

る。画像データはES(Video)1,ES(Video)2,ES(Video)3として示され、音声データはES(Audio)1,ES(Audio)2,ES(Audio)3として示されている。ECM1は画像データES(Video)1、音声データES(Audio)1に用いたスクランブル鍵のECMデータを示している。同様に、ECM2は画像データES(Video)2、音声データES(Audio)2に用いたスクランブル鍵のECMデータを示し、ECM3は画像データES(Video)3、音声データES(Audio)3に用いたスクランブル鍵のECMデータを示している。

【0056】NIT,PAT,PMT1,PMT2,PMT3は、PSIによるパケット化における制御データである。これらの制御データにより、各トランスポートストリームに含まれるチャンネル、時分割多重化されパケット化された3つのチャンネルの画像データ、音声データを識別することができる。制御データNIT,PAT,PMT1,PMT2,PMT3のデータ構造は、後に詳述する。

【0057】パケット化は、図4の縦線60aに示すように行われる。つまり、制御データNIT,PAT,PMT1,PMT2,PMT3、ECMデータECM1,ECM2,ECM3、画像データES(Video)1,ES(Video)2,ES(Video)3、音声データES(Audio)1,ES(Audio)2,ES(Audio)3の順にパケット化が行われる。音声データES(Audio)3までのパケット化が完了すれば、再び、制御データNIT以下のパケット化を繰り返す(縦線60b参照)。

【0058】画像データES(Video)1,ES(Video)2,ES(Video)3や音声データES(Audio)1,ES(Audio)2,ES(Audio)3は、制御データやECMデータに比べて大量に送られる。この実施形態では、固定長パケットを用いているので、画像データES(Video)1,ES(Video)2,ES(Video)3や音声データES(Audio)1,ES(Audio)2,ES(Audio)3は、制御データやECMデータに比べて多くのパケットが送られることとなる。図4において、画像データおよび音声データが太く示されているのは、このことを模式的に表したものである。

【0059】図5に、パケット化されたデータの基本的構造を示す。制御データ、ECMデータ、画像データ、音声データのいずれもが、図5に示すようなデータ構造を持つパケットとされる。パケット化データの先頭には、パケット符号PID(Packet ID)が付される。パケット符号PIDは、各パケットを識別するため各パケットごとにユニークに付された符号である。スクランブルコントロールビットは、当該パケットにスクランブルがかかっているか否か、スクランブルがかかっている場合には偶数鍵(Even)か奇数鍵(Odd)かを示す。たとえば、“00”はスクランブル無し、“10”は偶数鍵によるスクランブル、“11”は奇数鍵によるスクランブルを示す。内容データは、パケット化された対象データ(制御データ、ECMデータ、画像データ、音声データなど)である。

【0060】なお、この実施形態では、制御データNIT,PAT,PMT1,PMT2,PMT3やECMデータECM1,ECM2,ECM3にス

クランブルをかけないようにしている。したがって、これらデータのバケットにおいて、スクランブルコントロールビットは“00”となる。

【0061】図6に制御データPATのデータ構造を示し、図7に制御データPMT1、PMT2、PMT3のデータ構造を示す。制御データPMT1は、図7に示すように、画像データES(Audio)1のバケット符号PIDとそのスクランブル鍵のECMデータECM1のバケット符号PID、および音声データES(Audio)1のバケット符号PIDとそのスクランブル鍵のECMデータECM1のバケット符号PIDを有している。図7においては、画像データのECMデータのPIDが16進数で21、画像データのPIDが16進数で22、音声データのECMデータのPIDが16進数で21、音声データのPIDが16進数で24であることが示されている。なお、他のチャンネルの制御データPMT2、PMT3も同様の構成である。また、この実施形態では、画像データと音声データのスクランブル鍵を同じものとしたが、それぞれ異なるスクランブル鍵を用いるようにしてもよい。

【0062】制御データPATは、図6に示すように、各チャンネルの制御データPMT1、PMT2、PMT3のバケット符号PIDを示している。図6においては、3チャンネルのPMTのPIDが16進数で10、5チャンネルのPMTのPIDが16進数で11、7チャンネルのPMTのPIDが16進数で12であることが示されている。

【0063】図6、図7に示す制御データPAT、PMTによって、画像データ、音声データのバケットが、チャンネルごとに特定できる。

【0064】図8にECMデータECM1、ECM2、ECM3の構造を示す。ECMデータは、セクションヘッダとECM内容データとを有している。ECM内容データは、スクランブル鍵自体を暗号化したものである。セクションヘッダには、偶数鍵(Even)か奇数鍵(Odd)かを示すtable\_id、このECMデータによるスクランブル鍵が現在の鍵(カレント鍵という)か、次に用いる鍵(ネクスト鍵という)かを示すtable\_id\_extensionが設けられている。この実施形態では、table\_idが8進数で82であれば偶数鍵であること、83であれば奇数鍵であることを表す。また、table\_id\_extensionが00であれば、このECMデータがカレント鍵のものでありカレント鍵だけが送られていること、01であれば、このECMデータがカレント鍵のものであり同時にネクスト鍵も送られていること、10であれば、このECMデータがネクスト鍵のものであることを表している。

【0065】なお、この実施形態では、table\_id\_extensionによって上記の区別を行っている。しかしながら、ECMデータの内容に、このような区別を行うデータを記述するようにしてもよい。

【0066】以上のようにして、1つのトランスポンダに複数のチャンネルのデータが時分割で多重化され、1つ

のトランスポートストリームを形成している。なお、トランスポートストリームは複数設けられており、図9に示すようにその識別子Ts\_id、周波数・偏波方向などの伝送諸元、そのトランスポートストリームに含まれるチャンネルのリストがNIT(Network Information Table)データとして伝送される。

【0067】図10に、画像データES(Audio)1(または音声データES(Audio)1)とECMデータECM1の送出タイミングを示す。なお、図10の画像(音声)データにおいて、Odd0、Even1、Odd1、Even2と示した部分は、それぞれ、スクランブル鍵Odd0、Even1、Odd1、Even2によってスクランブルをかけた部分である。また、ECMデータECM1において、Odd0、Even1、Odd1、Even2と示した部分は、それぞれ、スクランブル鍵Odd0、Even1、Odd1、Even2の鍵対応データを送出している期間であることを示している。なお、他のチャンネルの画像データES(Audio)2、ES(Audio)2とECMデータECM2とのタイミング関係、画像データES(Audio)3、ES(Audio)3とECMデータECM3とのタイミング関係も、上記と同様である。

【0068】図4においては、ECMデータは1本のデータとして示されているが、より詳細には、図10に示すように、所定の重複期間では2つのECMデータが同時に送られている。図11に、重複期間の前後を拡大して示す。図11に示すように、画像(音声)データにおいて用いたスクランブル鍵がOdd0からEven1へ変わる時点Txより $\Delta t_1$ だけ早いタイミングTsにて、次のスクランブル鍵Even1の鍵対応データを送出している。

【0069】これは、受信装置において、鍵対応データからスクランブル鍵を復元するための時間を考慮して、画像や音声途切れることなく受信できるようにするためである。したがって、重複期間40の開始時Tsは下式のように定めるのが好ましい。

$$Ts = Tx - Rmax - \alpha$$

ここで、Txは暗号化データにおいて鍵の変わる時点を示す。Rmaxは、最大復元時間であり、想定される複数の受信装置において、連続して2つのECMデータを受けた時に、2つのスクランブル鍵に復元するために要する2重復元時間のうち、最も大きいものをいう。 $\alpha$ は余裕時間であり、0と等しいかそれ以上の値を持つ。

【0071】図15Aに示すように、1つずつしか復元処理をしない受信装置を想定する場合には、時点Q1から時点Q2までを2重復元時間とし、想定した各受信装置の2重復元時間のうち最も大きいものを最大復元時間Rmaxとする。

【0072】また、図15Bに示すように、2つの復元処理を並列して行う受信装置を想定する場合には、2つのECMデータを同時に与えてからスクランブル鍵を復元できるまでを2重復元時間とし、想定した各受信装置の2重復元時間のうち最も大きいものを最大復元時間Rmaxとする。

【0073】さらに、図15A、図15Bのような受信装置が混在することが想定される場合には、それぞれの最大復元時間のうち最も大きいものを全体としての最大復元時間 $R_{max}$ とする。

【0074】図11に戻って、暗号化データの暗号化に現在用いられているスクランブル鍵Odd0の鍵対応データは、次の鍵Even1の鍵対応データが送出され始めてからも、引き続き送出されている。したがって、この期間40は、現在の鍵Odd0の鍵対応データと次の鍵Even1の鍵対応データとが重複して送出されることとなる。現在の鍵Odd0の鍵対応データは、スクランブル鍵が変わる時点 $T_x$ より $\Delta t_2$ だけ早い時点 $T_e$ において、送出が停止される。

【0075】これは、受信側において、鍵対応データからスクランブル鍵を復元するための時間を考慮して、不要な鍵対応データを送出しないようにするためである。つまり、鍵対応データからスクランブル鍵Odd0が復元できた時点において、すでに使用されているスクランブル鍵が次のものEven1に変わっている場合には、その鍵対応データを送る必要はない。むしろ、鍵対応データを送ることによって、伝送路の実質的な伝送容量を低下させることとなる。したがって、重複期間40の終了時点 $T_e$ は下式のように定めるのが好ましい。

$$【0076】T_e = T_x - R_{min} + \beta$$

ここで、 $T_x$ は暗号化データにおいて鍵が変わる時点を示す。 $R_{min}$ は最小復元時間であり、想定される複数の受信装置において、連続して2つのECMデータを受けた場合に、2つのスクランブル鍵に復元するために要する2重復元時間のうち、最も小さいものをいう。 $\beta$ は余裕時間であり、0と等しいかそれ以上の値を持つ。

【0077】図15Aに示すように、1つずつしか復元処理をしない受信装置を想定する場合には、時点 $Q_1$ から時点 $Q_2$ までを2重復元時間とし、想定した各受信装置の2重復元時間のうち最も小さいものを最小復元時間 $R_{min}$ とする。

【0078】また、図15Bに示すように、2つの復元処理を並列して行う受信装置を想定する場合には、2つのECMデータを同時に与えてからスクランブル鍵を復元できるまでを2重復元時間とし、想定した各受信装置の2重復元時間のうち最も小さいものを最小復元時間 $R_{min}$ とする。

【0079】さらに、図15A、図15Bのような受信装置が混在することが想定される場合には、それぞれの最小復元時間のうち最も小さいものを全体としての最小復元時間 $R_{min}$ とする。

【0080】なお、 $R_{max}$ や $R_{min}$ を決定するために想定する受信装置として、可能性のある全ての受信装置を想定した場合には、全受信装置においてチャネル切換時の画像等の乱れを防止することができる。しかし、全受信装置に対して所定の割合（95%等）のものについて、チ

ヤネル切換時の画像等の乱れを防止することができるように受信装置を想定し、 $R_{max}$ や $R_{min}$ を決定してもよい。

### 【0081】(3)受信装置の構成

図12に、この実施形態による通信システムにおける受信装置のブロック図を示す。この実施形態においては、復調部64が受取手段32に該当し、ICカード80が鍵取得手段36に該当する。また、デ・スクランブラ68、トランスポートデコーダ70およびCPU72によって復号化手段34を実現している。

【0082】アンテナ62によって受信された電波は、復調部64において選択され、所望のトランスポートストリームのみがデジタルデータとして取り出される。誤り訂正部66は、パケットに付されている誤り訂正符号に基づいてデータの誤り訂正を行う。

【0083】デ・スクランブラ68は、スクランブル鍵に基づいて、トランスポートストリームのスクランブルを解除する。なお、パケットの中には制御データやECMデータの packets ようにスクランブルがかけられていないものも含まれる。スクランブルがかかっていないパケットの場合、デ・スクランブラ68は、何も処理を行わずそのままそのパケットを出力する。なお、スクランブルがかかっているか否かは、パケットのスクランブルコントロールビット（図5参照）を見ることにより判断することができる。

【0084】図13に、デ・スクランブラ68内に設けられているDSレジスタを示す。デ・スクランブラ68は、CPU72から与えられたスクランブル鍵と、そのスクランブル鍵を用いてスクランブルをかけられたパケットの符号PIDを、このDSレジスタに記憶する。なお、スクランブル鍵は、偶数鍵（Even鍵）と奇数鍵（Odd鍵）の2つが記憶されるようになっている。

【0085】デ・スクランブラ68は、与えられたパケットのスクランブルコントロールビット（図5参照）に基づいて、スクランブルされているか否かを判断する。スクランブルされていない場合には、誤り訂正部66からのトランスポートストリームをそのままトランスポートデコーダ70に与える。また、偶数鍵によってスクランブルされている場合には、当該パケットの偶数鍵をDSレジスタによって知り、その偶数鍵によってスクランブルを解除する。スクランブルの解除されたトランスポートストリームは、トランスポートデコーダ70に与えられる。奇数鍵によってスクランブルされている場合も同様である。

【0086】また、DSレジスタに必要なスクランブル鍵が記憶されていない場合（図のPIDが0x75であるパケットに対する偶数鍵を参照）には、スクランブルを解除することができないので、スクランブルされたままトランスポートデコーダ70に与える。

【0087】トランスポートデコーダ70は、デ・スクランブラ68からトランスポートストリームを受け、処

理部であるCPU72によって指定されたPIDを持つパケットのみを取り出す。この実施形態では、デ・スクランブラ68とトランスポートデコーダ70によって復元出力部が構成されている。

【0088】取り出されたパケットの内、画像データ、音声データは、ビデオデコーダ82、オーディオデコーダ84において圧縮が解凍され、アナログ信号に変換されて出力される。画像信号は、CRTコントローラ86によりNTSC画像信号に変換されて出力される。

【0089】CRTコントローラ86からのNTSC画像信号と、オーディオデコーダ84からの音声信号は、TVセット88に与えられる。したがって、TVセットのディスプレイ（図示せず）から画像が、スピーカ（図示せず）から音声出力される。

【0090】この実施形態では、受信装置本体90の出力はTVセット88に与えられている。しかしながら、アナログビデオレコーダ、デジタルビデオレコーダ、パーソナルコンピュータ等の他の機器に与えるようにしてもよい。パーソナルコンピュータやデジタルビデオデコーダ等のデジタル機器に出力する場合には、ビデオデコーダ82、オーディオデコーダ84において解凍した後のデジタルデータを与えるようにする。

【0091】トランスポートデコーダ70において取り出されたデータの内、制御データやECMデータは、記憶部であるメモリ74に記憶される。ECMデータはCPU72によって、コネクタ79を介して復元処理部であるICカード80に送られ、ICカード80はこのECMデータからスクランブル鍵を復元する。復元されたスクランブル鍵は、コネクタ79を介してCPU72に送り返される。CPU72は、これをデ・スクランブラ68に与える。なお、メモリ74には制御プログラムも格納されている。CPU72は、この制御プログラムにしたがって、各部を制御する。

【0092】操作パネル78は、操作者の操作により、チャンネル情報の入力等を行うためのものである。リモコン受光部76は、リモコン（図示せず）から送られてきたチャンネル情報等を受けるためのものである。

【0093】リモコン受光部76、操作パネル86からのチャンネル情報はCPU72に与えられる。CPU72はチャンネル情報を復調部64に与え、所望のチャンネルが属するトランスポートストリームのみを復調させる。また、受信した制御データに基づいて、トランスポートデコーダ70により、トランスポートストリームから所望のチャンネルのデータのみを取り出させる。

【0094】図14に、鍵取得手段であるICカード80の構成を示す。このICカード80は、受信装置本体90と接続するためのコネクタ94、データ伝送のためのインターフェイス96、CPU92、メモリ98を備えている。CPU92は、メモリ98に格納されたプログラムにしたがって、コネクタ94、インターフェイス

96を介して受け取ったECMデータに基づいてスクランブル鍵を復元する。

【0095】この実施形態におけるICカード80は、一度に1つのECMデータに対する復元処理を行う（図15A参照）。したがって、CPU72は、ECMデータをICカード80に送った後、ICカード80からスクランブル鍵が返送されて来るのを待って、次のECMデータをICカード80に送るようにしている。

【0096】(4)受信装置の動作

①鍵復元を1つずつ行う場合

図16、図17に、メモリ74に記憶された制御プログラムのフローチャートを示す。この制御プログラムは、受信装置本体90の電源投入またはチャンネルの切換により処理を開始する。以下、このフローチャートを参照しつつ受信装置の動作を説明する。

【0097】まず、ステップS1において、CPU72は電源投入であるかチャンネル切換であるかを判断する。操作パネル78またはリモコン受光部76より新たなチャンネル情報（所望のチャンネルを示す情報）が与えられた場合には、チャンネル切換であると判断できる。また、リセット動作が行われることにより、電源投入であると判断できる。

【0098】チャンネル切換であった場合には、現在受信しているトランスポートストリームに所望のチャンネルが含まれているかどうかを判断する。この判断は、受信した制御データNITの内容を見ることによって行うことができる（図4および図9参照）。

【0099】現在受信中のトランスポートストリーム内に所望のチャンネルが含まれていない場合、CPU72は、図9に示す制御データNITの内容にしたがって所望のチャンネルが含まれるトランスポートストリームの識別子Ts\_id、伝送諸元を取得する。CPU72は、取得したトランスポートストリームの識別子Ts\_id、伝送諸元を復調部64に与える（ステップS3）。復調部64は、与えられた識別子Ts\_id、伝送諸元にもとづいて、所望のトランスポートストリームのみを選択的に復調して出力する。これにより、誤り訂正部66によって誤り訂正されたトランスポートストリームが、デ・スクランブラ68に与えられる。CPU72は、ステップS4の処理に進む。

【0100】なお、現在受信しているトランスポートストリーム内に所望のチャンネルが含まれている場合には、復調部64の切換を行う必要がないので、CPU72は、ただちにステップS4の処理に進む。

【0101】また、電源投入の場合には現在受信中のトランスポートストリームが存在しないので、CPU72は復調部64の切換を行った後、ステップS4の処理に進む。

【0102】ステップS4において、CPU72は、トランスポートデコーダ70に、制御データPATのパケッ

ト符号PIDを設定する。これにより、トランスポートデコード70は、トランスポートストリームから制御データPATを取り出して、メモリ74に記憶する。

【0103】次に、CPU72は、メモリ74に記憶された制御データPATに基づいて、所望のチャンネルの制御データPMTのパケット符号PIDを取得する（図6参照）。図6の例でいえば、3チャンネルを受信するのであれば、3チャンネルの制御データPMTのパケット符号PIDが16進数で“10”であることがわかる。

【0104】続けて、CPU72は、トランスポートデコード70に、所望のチャンネルの制御データPMTのパケット符号PIDを設定する。これにより、トランスポートデコード70は、トランスポートストリームから所望のチャンネルの制御データPMTを取り出して、メモリ74に記憶する。

【0105】さらに、CPU72は、メモリ74に記憶された制御データPMTに基づいて、所望のチャンネルの画像データ、音声データ、ECMデータの packets 符号PIDを取得する（図7参照）。CPU72は、取得した packets 符号PIDに基づいて、画像データ、音声データを取得するようにトランスポートデコード70を制御し、ECMデータからスクランブル鍵を復元させるようにICカード80を制御し、スクランブル鍵によって画像データ、音声データのスクランブルを解除するようにデ・スクランブラ68を制御する（ステップS6）。

【0106】ステップS6における処理の詳細を図17に示す。ここでは、図18の時点X1において、チャンネルの切換または電源投入があって、このチャンネルに対する処理が開始されたものとして説明を進める。

【0107】まず、所望のチャンネルの画像、音声データのスクランブル鍵に対応するECMデータの packets 符号PIDを、トランスポートデコード70に設定する（ステップS11）。これにより、トランスポートデコード70は、設定されたPIDを持つECMデータ（つまり所望のチャンネルの画像、音声データのスクランブル鍵のECMデータ）を選択的に取り出してメモリ74に記憶する。

【0108】さらに、CPU72は、取得したECMデータのtable\_idおよびtable\_id\_extensionを読んで、必要としているECMデータであるか否かを判断する（ステップS11）。このような判断を行うのは、一度取得したECMデータはもはや取得する必要がないので、新たなECMデータのみを取得するようにするためである。具体的には、必要とするECMデータのtable\_id、table\_id\_extensionを指定することによってこの判断を行うが、その詳細については後述する。なお、処理開始時には、必要とするECMデータのtable\_id、table\_id\_extensionの指定は行わないので、packets 符号PIDによって指定したECMデータであれば、無条件で指定条件を満たしたものとみなされる。

【0109】指定条件を満たさないECMデータである場合には、再び、ECMデータの取得を繰り返す。指定条件を満たすECMデータである場合には、当該ECMデータをICカード80に送る（ステップS12）。つまり、図18の時点X1において、スクランブル鍵Odd0のECMデータをICカード80に送る。ECMデータを受け取ったICカード80は、このECMデータからスクランブル鍵Odd0を復元し、時点X2においてCPU72に送り返す（ステップS13）。

【0110】スクランブル鍵Odd0を受け取ったCPU72は、スクランブル鍵Odd0をデ・スクランブラ68に設定する。これにより、デ・スクランブラ68は、画像および音声データのスクランブルを解除してトランスポートデコード70に出力するようになる。

【0111】ECMデータには、図8に示すようにtable\_id\_extensionとして、カレントのみ、カレント（ネクスト有り）、ネクストの3つの区別が付されている。これにより、CPU72は、受け取った鍵が、図10のaの期間（カレントのみ）にあるのか、bの期間（カレント（ネクスト有り））にあるのか、cの期間（ネクスト）にあるのかを知ることができる。なお、dに示す期間は、Even1鍵にとって、本来、ネクストとすべきであるが、この実施形態ではカレントとして扱っている。

【0112】CPU72は、table\_id\_extensionに基づいて、ICカード80から受け取った鍵がカレント鍵（現在使われている鍵）であるか、ネクスト鍵（次に使われる鍵）であるかを判断する（ステップS15）。スクランブル鍵Odd0のECMデータのtable\_id\_extensionには、カレント鍵である旨の区別が付されているので、CPU72はステップS16に進む。

【0113】ステップS16においては、X1の時点において、ネクスト鍵が同時に送られてきていたか否かを判断する。これも、スクランブル鍵Odd0のECMデータのtable\_id\_extensionによって判断することができる。時点X1においては、カレント鍵のみであって、ネクスト鍵はまだ送信されていないことがtable\_id\_extensionよりわかるので、ステップS17に進む。ステップS17においては、トランスポートデコード70に、所望のチャンネルの画像データ、音声データの packets 符号PIDが設定されているかどうかを判断する。現在、まだ画像データ、音声データのPIDは設定していないので、ステップS18に進む。

【0114】ステップS18において、CPU72は、すでにステップS5において取得している所望のチャンネルの画像データ、音声データの packets 符号PIDを、トランスポートデコード70に設定する。これにより、トランスポートデコード70は、所望のチャンネルの画像データ、音声データを、ビデオデコード82、オーディオデコード84に出力し始める。すなわち、図18の場合には、時点X1にてチャンネル切換が行われてから、ICカ

ード80による復元処理時間経過後の時点X2より、画像および音声はTVセット88から出力される。時点X1にチャンネル切換があれば、時点X2において、画像・音声は立ち上がる。

【0115】次に、CPU72は、ステップS11における受信すべきECMデータの設定を変更する（ステップS19）。これは、現在の鍵Odd0は既に取得したので、次の鍵Even1を取得ように設定するためである。ここでは、今回取得したECMデータと異なったtable\_id（つまり偶数鍵）を持ったECMデータを取得するように設定する。なお、table\_idは、図8に示すように、偶数鍵、奇数鍵によって異なるようになっている。その後、ステップS11に戻って処理を繰り返す。

【0116】この実施形態では、table\_idによって、すでにその鍵を取得したかどうかを判断するようにしているが、セクションヘッダ中のバージョン情報によって判断するようにしてもよい。この場合、異なるECMデータには、異なるバージョン情報を付しておくようにする。

【0117】次に、ネクスト鍵Even1のECMデータを取得すると（ステップS12、図18の時点X3）、ICカード80によってネクスト鍵Even1を得る（ステップS13、時点X4）。CPU72は、これをデ・スクランブラ68に設定する（ステップS14）。このようにして、ネクスト鍵Even1によってスクランブルされた画像データ、音声データが送られてくる前に、ネクスト鍵Even1をデ・スクランブラ68に設定するので、画像および音声データを途切れることなく出力することができる。

【0118】次に、CPU72は、トランスポートデコーダ70に、画像データ、音声データのPIDが設定されているかを判断する（ステップS20）。ここでは、すでにPIDが設定されているので、ステップS21に進んで、取得するECMデータの設定を変更する。

【0119】ステップS21においては、今回取得したECMデータと異なったtable\_idを持ち、ネクストのtable\_id\_extensionを持ったECMデータを取得するように設定する。その後、ステップS11に戻って処理を繰り返す。

【0120】以後は、順次上記の処理を繰り返して、TVセット88にNTSC画像信号と音声信号を出力する。

【0121】なお、図19に示すように、チャンネル切換の時点X1が重複期間40の開始時点に近接している場合には、ネクスト鍵Even1のECMデータが送られてきていても、ICカード80がカレント鍵Odd0の復元処理を行っている状態となる。したがって、ネクスト鍵Even1の復元処理は、カレント鍵Odd0の復元処理が終わってから（時点X2、X3参照）ということになり、ネクスト鍵Even1の取得が後ろにずれ込むこととなる。

【0122】しかしながら、図19のΔt1は、最も遅い処理の受信装置における2重復元時間（2つのECMデータから連続して2つのスクランブル鍵を復元するに要する時間）を基準として設定されているので、スクランブル鍵が変わる時点Txよりも早くネクスト鍵Even1をデ・スクランブラ68に設定することができる。つまり、画像および音声は途切れることなく出力される。したがって、図19に示す場合も、図18と同じように、時点X1にてチャンネル切換が行われてから、ICカード80による復元処理時間経過後の時点X2に、画像および音声は立ち上がる。つまり、画像および音声をTVセット88から得ることができる。

【0123】次に、図20に示すように、時点X1においてチャンネルの切換または電源投入があつて、このチャンネルに対する処理が開始された場合の処理を説明する。時点X1は重複期間40内にあるので、カレントの鍵Odd0のECMデータとネクストの鍵Even1のECMデータが送られてきている。

【0124】CPU72は、取得したECMデータのtable\_id\_extensionから、そのECMデータによる鍵が、カレント鍵（ネクストあり）か、ネクスト鍵かを判断することができる（図8参照）。先に、時点X1において、カレント鍵Odd0のECMデータを取得した場合には、時点X2においてカレント鍵Odd0をICカード80から得る。CPU72は、当該カレント鍵Odd0をデ・スクランブラ68に設定した後、ステップS15を経て、ステップS16に進む。ここでは、（ネクストあり）であるから、ステップS19に進んで、取得するECMデータの設定を変更する。ここでは、異なるtable\_idのECMデータを（つまり偶数鍵のECMデータ）を指定し、ステップS11以下を実行する。

【0125】指定した偶数鍵（つまりネクスト鍵Even1）のECMデータを取得すると（時点X3）、これをICカード80に送って、ネクスト鍵Even1を得る（時点X4）。CPU72は、これをデ・スクランブラ68に設定する（ステップS14）。次に、ステップS15を経て、デコーダ70に音声・画像のPIDを設定済みかどうかを判断する（ステップS20）。ここではまだ設定していないので、ステップS18に進み、所望のチャンネルの画像データ、音声データのバケット符号PIDをトランスポートデコーダ70に設定し、デコードを開始する。つまり、図20の場合には、時点X1のチャンネル切換に対し、時点X4から画像、音声は立ち上がる。

【0126】上記のように、重複期間40内においてチャンネル切換等によって当該チャンネルに対する処理を開始した場合には、カレント鍵だけが取得できた時点X2ではデコードを開始せず（PIDを設定せず）、ネクスト鍵が得られてはじめてデコードを開始し（PIDを設定し）、画像データ、音声データを出力するようにしている。



【0127】上記のように処理している理由を、図21を用いて説明する。図21に示すような場合において、カレント鍵Odd0だけが取得できた時点X2からデコードを開始すると、区間R1で画像・音声を得られた後、区間R2で画像・音声途切れという問題を生じる。これは、区間R2ではネクスト鍵Even1がまだ取得できていないためである。

【0128】したがって、重複期間40内において当該チャンネルの処理を開始した場合には、ネクスト鍵が得られてから音声・画像のPIDをデコーダ70に設定するようにしている。その結果、図21の場合であれば、時点X4から画像・音声出力が得られることとなり、画像や音声の途切れがない。

【0129】なお、図20の場合において、時点X1で先にネクスト鍵Even1のECMデータを取得し、時点X2でネクスト鍵Even1が得られた場合には、ステップS15、S20を経て、トランスポートデコーダ70に画像および音声のバケット符号PIDを設定する（ステップS18）。つまり、カレント鍵Odd0の取得を待たずに、デコーダ70への設定を行う。しかし、ネクスト鍵Even1によってスクランブルされた画像および音声データはまだ送られてきていないので、設定したバケット符号PIDに対応する画像および音声データが直ちに出力されるものではない。

【0130】その後、時点X4にてカレント鍵Odd0を取得した時点で、現在送られてきている画像および音声データのスクランブルを解除することができ、画像および音声出力される。したがって、結果的に、時点X4から画像および音声を得られる点は同じである。

【0131】また、図21の場合において、時点X1で先にネクスト鍵Even1のECMデータを取得し、時点X2でネクスト鍵Even1が得られた場合には、ステップS15、S20を経て、トランスポートデコーダ70に画像および音声のバケット符号PIDを設定する（ステップS18）。つまり、カレント鍵Odd0の取得を待たずに、デコーダ70への設定を行う。しかし、ネクスト鍵Even1によってスクランブルされた画像および音声データはまだ送られてきていないので、設定したバケット符号PIDに対応する画像および音声データが直ちに出力されるものではない。

【0132】その後、ネクスト鍵Even1によってスクランブルがかけられた画像および音声データが送られてくる時点Txより、画像および音声データが出力されることとなる。なお、このケースの場合には、時点X4にて復元されたOdd0鍵は使用されない。

【0133】いずれにしても、この実施形態では、重複期間40においてチャンネル切換等によって処理を開始した場合、少なくともネクスト鍵が取得できた後に、デコードを開始して、画像および音声データを出力するようにしている。したがって、図21に示すような状況にお

いても、一旦出力された画像および音声データが途切れるおそれがない。

【0134】次に、図22に示すように、時点X1においてチャンネル切換等があった場合について説明する。この場合には、時点X1においてECMデータを取得し、時点X2において復元した鍵Even1を得る。その後、ステップS15、S20を経て、ステップS18においてデコードを開始する。したがって、時点X2より、画像および音声データの出力が得られる。

【0135】上記のようにこの実施形態においては、図20や図21に示す場合を除いて、チャンネルの切換等から画像・音声を得られるまでの立ち上がり時間を、鍵復元に要する時間と等しくすることができる。ただし、図20や図21の場合には、最悪、鍵復元に要する時間の2倍の時間を要することとなる。

【0136】図20の場合においても、復元処理の速い受信装置については、チャンネルの切換等から画像・音声を得られるまでの立ち上がり時間を、鍵復元に要する時間と等しくすることが可能である。

【0137】そのためには、図20のカレント鍵Odd0が取得できた時点X2において、下記の2つの条件を満足するか否かを判断し、満足している場合には、時点X2において画像・音声のPIDをデコーダ70に設定して、デコードを開始するようにすればよい。

【0138】条件1：時点X2が重複期間40内にあること。

【0139】条件2： $\Delta t2 > \Delta tr$ を満たすこと。

【0140】ここで、 $\Delta t2$ は重複期間40の終了Teから鍵の切り替わる時点Txまでの時間、 $\Delta tr$ はこの受信装置による復元時間（ECMデータからスクランブル鍵を復元するのに必要な時間）である。

【0141】条件1、2をとともに満足する場合には、時点X2からデコードを開始し、画像および音声データを出力しても、以後、途切れることなく画像および音声データを出力することができる。したがって、このような判断を行うことにより、チャンネル切換から画像および音声出力までの立ち上がり時間を短くすることができる。

【0142】なお、上記のような処理を行うためには、受信装置側において $\Delta t2$ の大きさが知られていなければならない。通信システムとして、 $\Delta t2$ が予め固定されている場合は、その値を受信装置に予め設定しておけばよい。また、 $\Delta t2$ が固定されていない場合には、送信装置から $\Delta t2$ の値を受信装置に送るようにすればよい。

【0143】②2つの鍵復元を同時に並行して行う場合  
上記では、受信装置における鍵の復元処理が、1つのECMデータごとに行われる場合について説明した。しかし、受信装置における鍵の復元処理が、図15Bに示すように並行して行われる場合には、図17の処理に換えて、図23、図24に示すような処理を行えばよい。

【0144】まず、図25の時点X1において、チャンネル



の切換または電源投入があって、このチャンネルに対する処理が開始された場合について説明する。

【0145】まず、CPU72は、所望のチャンネルの画像、音声データのスクランブル鍵に対応するECMデータのバケット符号PIDを、トランスポートデコーダ70に設定し（ステップS51）、当該ECMデータを選択的に取り出してメモリ74に記憶する。

【0146】さらに、CPU72は、取得したECMデータのtable\_idおよびtable\_id\_extensionを読んで、必要としているECMデータであるか否かを判断する（ステップS51）。なお、処理開始時には、必要とするECMデータのtable\_id、table\_id\_extensionの指定は行わないので、バケット符号PIDによって指定したECMデータであれば、無条件で指定条件を満たしたものとみなされる。

【0147】したがって、図25の時点X1において、スクランブル鍵Odd0のECMデータを取得し、ステップS52に進む。ステップS52、S54では、取得したECMデータのtable\_id\_extensionを見て、受信したECMデータが“カレント（ネクストあり）”か“ネクスト”であるかを判断する。つまり、重複期間40内における受信であるかどうかを判断する。ここでは、重複期間40外の受信であるから、ステップS58に進む。

【0148】ステップS58においては、ECMデータをICカード80に送る。ECMデータを受け取ったICカード80は、このECMデータからスクランブル鍵Odd0を復元し、時点X2においてCPU72に送り返す（図24、ステップS59）。

【0149】スクランブル鍵Odd0を受け取ったCPU72は、スクランブル鍵Odd0をデ・スクランブラ68に設定する（ステップS60）。これにより、デ・スクランブラ68は、画像および音声データのスクランブルを解除してトランスポートデコーダ70に出力するようになる。次に、トランスポートデコーダ70に、所望のチャンネルの画像データ、音声データのバケット符号PIDが設定されているかどうかを判断する（ステップS61）。ここでは、まだ設定していないので、ステップS62に進み、所望のチャンネルの画像データ、音声データのバケット符号PIDをトランスポートデコーダ70に設定する。

【0150】これにより、トランスポートデコーダ70は、所望のチャンネルの画像データ、音声データを、ビデオデコーダ82、オーディオデコーダ84に出力し始める。すなわち、図25の場合には、時点X1にてチャンネル切換が行われてから、ICカード80による復元処理時間経過後の時点X2より、画像および音声信号がTVセット88から出力される。

【0151】次に、CPU72は、ECMデータのtable\_id\_extensionが“カレント（ネクスト無し）”であったかどうかを判断する（ステップS63）。ここで

は、“カレント（ネクスト無し）”であるから、ステップS64に進み、受信すべきECMデータの変更を行う。ここでは、今回取得したECMデータと異なったtable\_id（つまり偶数鍵）を持ち、table\_id\_extensionが“ネクスト”であるECMデータを取得するように設定する。

【0152】次に、ネクスト鍵Even1のECMデータを取得すると（ステップS51、図25の時点X3）、ステップS52、S54、S55を経てステップS58に進む。ステップS58、S59においては、ICカード80にECMデータを送信し、ネクスト鍵Even1を得る（時点X4）。CPU72は、これをデ・スクランブラ68に設定する（ステップS60）。このようにして、ネクスト鍵Even1によってスクランブルされた画像データ、音声データが送られてくる前に、ネクスト鍵Even1をデ・スクランブラ68に設定するので、画像および音声データを途切れることなく出力することができる。

【0153】次に、CPU72は、トランスポートデコーダ70によって画像データ、音声データのデコードが開始されているか否かを判断する（ステップS20）。ここでは、すでにデコードが開始されているので、ステップS63を経て、ステップS65に進んで、取得するECMデータの設定を変更する。

【0154】ステップS65においては、カレントのECM（つまり時点X1にて受信したECM）のTable\_id（つまり奇数鍵）を持ち、“ネクスト”のTable\_id\_extensionを持つECMを受信するように設定する。その後、ステップS51に戻って処理を繰り返す。

【0155】以後は、順次上記の処理を繰り返して、TVセット88にNTSC画像信号と音声信号を出力する。

【0156】なお、図26に示すように、チャンネル切換の時点X1が重複期間40の開始時点に近接している場合には、ネクスト鍵Even1のECMデータが送られてきているにもかかわらず、ICカード80がカレント鍵Odd0の復元処理を行っている状態となる。したがって、ネクスト鍵Even1の復元処理は、カレント鍵Odd0の復元処理が終わってから（時点X2、X3参照）ということになり、ネクスト鍵Even1の取得が後ろにずれ込むこととなる。

【0157】しかしながら、図19のΔt1は、最も遅い処理の受信装置における2重復元時間（2つのECMデータから連続して2つのスクランブル鍵を復元するに要する時間）を基準として設定されているので、スクランブル鍵が変わる時点Txよりも早くネクスト鍵Even1をデ・スクランブラ68に設定することができる。つまり、画像および音声信号が途切れることなく出力される。したがって、図26に示す場合も、図25と同じように、時点X1にてチャンネル切換が行われてから、ICカード80による復元処理時間経過後の時点X2より、画像および音声信号がTVセット88から得ることができる。

【0158】次に、図2.7に示すように、時点X1においてチャンネルの切換または電源投入があって、このチャンネルに対する処理が開始された場合の処理を説明する。時点X1は重複期間40内にあるので、カレントの鍵Odd0のECMデータとネクストの鍵Even1のECMデータが送られてきている。

【0159】CPU72は、取得したECMデータのtable\_id\_extensionから、そのECMデータによる鍵が、カレント鍵（ネクストあり）か、ネクスト鍵かを判断することができる（図8参照）。先に、時点X1においてカレント鍵Odd0のECMデータを取得した場合には、ステップS52、S53を経て、ステップS56において、異なるTable\_id（つまりEven鍵）を持つECMデータを受信するように設定する。このようにして、2つのECMデータを受信した後、これらをICカードに送信する（ステップS58）。この実施形態では、ICカード80は、2つの鍵の復元処理を同時に行うことができるので、CPU72は同時に2つの鍵を受け取る（時点X2）。したがって、時点X2から画像・音声の出力が得られる。

【0160】なお、CPU72からICカード80へのECMデータの伝送（伝送のための前処理や後処理を含む）、復元した鍵の伝送（伝送のための前処理や後処理を含む）には時間を要する。したがって、この実施形態のように同時処理を行うことのできるICカードを用いることにより、CPU72がECMデータを受け取ってから、復元した鍵を得るまでの立ち上がり時間を短くすることができる。つまり、チャンネル切換時等に映像・音声を得るまでの時間を短くすることができる。

【0161】次に、図2.8に示すように、時点X1においてチャンネル切換等があった場合について説明する。この場合には、時点X1においてECMデータを取得し、ステップS52、S54、S58を経て、時点X2において復元した鍵Even1を得る。その後、ステップS62においてESのPIDを設定し、デコードを開始する。したがって、時点X2より、画像および音声データの出力が得られる。

【0162】なお、この実施形態では、図2.6に示すような場合において、Odd0の鍵が復元されるのを待って、Even1の鍵の復元処理を行っている。しかし、重複期間40の開始時点Tsより、Even1の鍵の復元処理を並行して行うようにしてもよい。2つの鍵の復元を同時に行った方が、それぞれ単独で処理するよりも速いようなICカード80を用いる場合には、並行処理を行うことにより、重複期間40を短くすることができる。

【0163】3. 衛星放送システムにおける第2の実施形態

図2.9に、他の実施形態におけるECMデータの送出タイミングを示す。この実施形態では、重複期間40において、2つのスクランブル鍵を1つのECMデータとし

て送出するようにしている。したがって、重複期間40以外では1つのECMデータに1つのスクランブル鍵が含まれ、重複期間40では1つのECMデータに2つのスクランブル鍵が含まれることとなる。

【0164】図3.0に、この実施形態におけるECMデータの構造を示す。table\_id\_extensionには、図2.3の①②③④を区別する情報が記述されている。table\_id\_extensionが①③を示している場合には1つのECMデータが含まれ、②④を示している場合には2つのECMデータが含まれる。なお、この実施形態では、table\_idは常に同一であり、奇数鍵、偶数鍵の区別をしていない。table\_id\_extensionのほうに、この情報が含まれているからである。

【0165】図3.1に、重複期間40近傍の拡大図を示す。重複期間40の開始時点Tsは下式のように定めるのが好ましい。

$$【0166】Ts = Tx - Rmax - \alpha$$

ここで、Txは暗号化データにおいて鍵の変わる時点を示す。Rmaxは、最大復元時間であり、想定される受信装置において1つのECMデータから1つのスクランブル鍵を復元するために要する復元時間と、1つのECMデータから2つのスクランブル鍵を復元するために要する復元時間との合計を合計復元時間としたとき、想定される複数の受信装置において最も大きい合計復元時間をいう。αは余裕時間であり、0と等しいかそれ以上の値を持つ。

【0167】上記のように最大復元時間Rmaxを定めたのは、図3.5に示すように、重複期間40の直前の時点X1においてチャンネル切換等があった場合を考慮したものである。この場合、復元によって鍵Odd0が得られた時点X2にて画像および音声データの出力を開始しても、スクランブル鍵が変わる時点Txより前に、ネクスト鍵Even1を取得することが保証される。これは、Δt1を、最も復元処理の遅い受信装置における合計復元時間以上に設定しているからである。

【0168】また、重複期間40の終了時点Teは下式のように定めるのが好ましい。

$$【0169】Te = Tx - Rmin + \beta$$

ここで、Txは暗号化データにおいて鍵の変わる時点を示す。Rminは最小復元時間であり、想定される受信装置において1つのECMデータから1つのスクランブル鍵を復元するために要する復元時間と、1つのECMデータから2つのスクランブル鍵を復元するために要する復元時間との合計を合計復元時間としたとき、想定される複数の受信装置において最も小さい合計復元時間をいう。βは余裕時間であり、0と等しいかそれ以上の値を持つ。

【0170】この実施形態において用いる受信装置のブロック図は図1.2に示すものと同じである。さらに、メモリ74に記憶された受信処理プログラムのフローチャ

ートも、図16に示す概略は同様である。しかし、図16のステップS6のECM、ESの受信に関する処理の詳細が異なる。図32に、この実施形態によるECM、ESの受信処理プログラムをフローチャートにて示す。

【0171】図33に、この実施形態において用いる鍵再生装置102の全体構成を示す。この鍵再生装置102は、個数検出手段104と鍵再生手段106を備えている。個数検出手段104は、与えられた鍵対応データ中に何個の鍵が含まれているかを検出する。鍵再生手段106は、個数検出手段によって検出された個数の鍵を、鍵対応データから復元する。

【0172】この鍵再生装置102を、CPUを用いてICカードとして実現した場合のハードウェア構成は、図14に示すものと同じである。図34に、ICカード80のメモリ98に記録された処理プログラムのフローチャートを示す。

【0173】以下、図32、図34を参照して、この実施形態による受信装置90の動作を説明する。

【0174】まず、CPU72は、所望のチャンネルの画像、音声データのスクランブル鍵に対応するECMデータのバケット符号PIDを、トランスポートデコーダ70に設定する(ステップS31)。これにより、トランスポートデコーダ70は、設定されたPIDを持つECMデータ(つまり所望のチャンネルの画像、音声データのスクランブル鍵のECMデータ)を選択的に取り出してメモリ74に記憶する。

【0175】さらに、CPU72は、取得したECMデータのtable\_id\_extensionを読んで、指定されたtable\_id\_extensionであるか否かを判断する。指定したtable\_id\_extensionを持ったECMデータでない場合には、受信を繰り返す。指定したtable\_id\_extensionを持ったECMデータであれば、ステップS32に進む。ただし、チャンネル切換時や電源投入時等の当該チャンネルに対する処理開始時には、table\_id\_extensionを指定しないので、設定されたPIDを持つECMデータを受信すれば、ステップS32に進むこととなる。

【0176】ステップS32において、CPU72は、ECMデータをICカード80に送信する。ICカード80は、図34のフローチャートに示すように、与えられたECMデータに2つの鍵が含まれているか否かを判断する(ステップS41)。この判断は、CPU72から送られてくるtable\_id\_extensionや全体のデータ長等によって判断することができる。

【0177】2つの鍵が含まれている場合には2つの鍵を復元して送り返し(ステップS42)、1つの鍵が含まれている場合には1つの鍵を復元して送り返し(ステップS43)。なお、2つの鍵を送り返す場合には、何れが偶数鍵であり、何れが奇数鍵であるかを明らかにして送り返す。

【0178】図34に戻って、ステップS33において

スクランブル鍵を受け取ったCPU72は、それがカレントの鍵であるかどうかを判断する。この判断は、当該鍵のECMデータ中のtable\_id\_extensionによって行うことができる。また、2つの鍵が含まれている場合には、先に現れるECMデータ(図30のECM1)がカレント鍵であると定める等の方法により、いずれがカレント鍵かネクスト鍵かが分かるようにしている。

【0179】table\_id\_extensionには、図29の①②③④を区別するための情報が記述されている。これにより、①②においてはカレント鍵が偶数鍵、③④においてはカレント鍵が奇数鍵であることを知ることができる。したがって、CPU72は、このtable\_id\_extensionに基づいて、受け取った鍵がカレント鍵であるか否か、あるいは、2つの鍵を受け取った場合には何れがカレント鍵であるかを知ることができる。

【0180】CPU72は、カレント鍵を受け取った場合には、これをデ・スクランブラ68のDSデコーダに設定する(図13参照)。これにより、デ・スクランブラ68は、画像および音声データのスクランブルを解除して、トランスポートデコーダ70に与える。

【0181】次に、CPU72は、table\_id\_extensionに基づいて、ネクスト鍵が送られてきているか否か、つまり②④であるかどうかを判断する(ステップS35)。ネクスト鍵が送られてきていなければ、つまり①③であれば、重複期間40内ではないので、ステップS37を経て、トランスポートデコーダ70に、所望のチャンネルの画像データ、音声データのバケット符号PIDを設定する(ステップS38)。これにより、トランスポートデコーダ70は、所望のチャンネルの画像データ、音声データを、ビデオデコーダ82、オーディオデコーダ84に出力し始める。

【0182】次に、CPU72は、取得すべきECMデータのtable\_id\_extensionを指定した後、ステップS31に戻る。現在取得したECMデータのtable\_id\_extensionが①または④であれば、②または③を取得するように指定する。現在取得したECMデータのtable\_id\_extensionが②または③であれば、①または④を取得するように指定する。この指定によって、ステップS31において、一度取得して必要のないECMデータを受信した場合には、ステップS32以下に進まないようにしている。

【0183】以上のように、重複期間40内にチャンネル切換等によって処理を開始し、ECMデータを受け取った場合には、カレント鍵とネクスト鍵をデ・スクランブラに設定した後、デコードを開始するようにしている。また、重複期間40外で処理を開始し、ECMデータを受け取った場合には、カレント鍵をデ・スクランブラに設定した後、デコードを開始するようにしている。なお、重複期間40の終了時点Teから鍵が変わる時点Tx間での間は、ネクスト鍵が送られているが、table\_id\_ext

ensionではカレント鍵を送っているものとし、図32における処理もこのtable\_id\_extensionに従うようにしている。

【0184】なお、この実施形態において、 $\Delta t1$ は、想定される最も復元処理の遅い受信装置において1つのECMデータから1つのスクランブル鍵を復元するために要する復元時間と、1つのECMデータから2つのスクランブル鍵を復元するために要する復元時間との合計復元時間である最大復元時間 $R_{max}$ と等しいかまたはそれ以上に設定されている。したがって、図35に示すように、重複期間40の直前にチャネル切換等があった場合、いずれの受信装置においても、鍵が変わる時点 $T_x$ より前にネクスト鍵を取得することができる。したがって、カレント鍵Odd0を取得した時点 $X2$ において画像および音声データを出力しても、途切れることなく画像および音声データを出力することができる。

【0185】一般的に、2つのECMデータを受けて2つの鍵を復元する時間よりも、2つの鍵が含まれた1つのECMデータから2つの鍵を復元する時間の方が短い。これは、前者の場合には、ECMデータをICカードに送る処理、および復元された鍵を受信装置30のCPU72に送り返す処理を2回行わねばならず、その時間を要するからである。したがって、図20に示すように、重複期間40内においてチャネル切換等があった場合には、図16、図17に示す実施形態よりも、本実施形態の方が立ち上がり時間が短くなる。

【0186】なお、上記実施形態では、図29の③にてカレント鍵Odd0を復元して取得した後、④にてカレント鍵Odd0とネクスト鍵Even1の双方を復元して取得するようにしている。したがって、すでに、取得済みのカレント鍵Odd0の復元を行っており、その分だけ復元時間が長くなっていた。これを解決するため、図36に示すように、カレント鍵が取得済みである場合には、2つの鍵が含まれたECMデータを取得した場合であっても、ICカード80にてネクスト鍵だけを復元するように指示してもよい（ステップS31C）。これにより、鍵の復元時間を短くすることができる。

【0187】以上のような処理を行うことにより、図35に示すような場合に、時点 $X3$ にてECMデータを取得してから、復元が完了する時点 $X4$ までの時間が短縮される。したがって、重複期間40の開始時点 $T_s$ を下式のように決定することができる。

$$【0188】 T_s = T_x - R_{max} - \alpha$$

ここで、 $T_x$ は暗号化データにおいて鍵が変わる時点を示す。 $R_{max}$ は、最大復元時間であり、想定される受信装置において1つのECMデータから1つのスクランブル鍵を復元するために要する復元時間と、2つのスクランブル鍵を含む1つのECMデータから1つのスクランブル鍵を復元するために要する復元時間との合計を合計復元時間としたとき、想定される複数の受信装置において最

も大きい合計復元時間をいう。 $\alpha$ は余裕時間であり、0と等しいかそれ以上の値を持つ。

【0189】上記のように、 $R_{max}$ を図32の実施形態に比べて小さくすることができるので、重複期間40の開始時期を後ろにずらすことができる。これにより、重複期間40を小さくして、ECMデータの送信密度を減らすことができる。

【0190】また、重複期間40の終了時点 $T_e$ を下式のように決定することができる。

$$【0191】 T_e = T_x - R_{min} + \beta$$

ここで、 $T_x$ は暗号化データにおいて鍵が変わる時点を示す。 $R_{min}$ は、最小復元時間であり、想定される受信装置において1つのECMデータから1つのスクランブル鍵を復元するために要する復元時間と、2つのスクランブル鍵を含む1つのECMデータから1つのスクランブル鍵を復元するために要する復元時間との合計を合計復元時間としたとき、想定される複数の受信装置において最も小さい合計復元時間をいう。 $\beta$ は余裕時間であり、0と等しいかそれ以上の値を持つ。

【0192】上記のように、 $R_{min}$ を前記の実施形態に比べて小さくすることができるので、重複期間40の終了時期を鍵が変わる時点 $T_x$ に近づけることができる。これにより、処理の迅速な受信装置において、重複期間40終了直前でチャネル切換があった場合の立ち上がり時間を短くすることができる。

【0193】なお、 $T_e$ が後ろにずれることにより重複期間40が長くなるが、これは、 $T_s$ が後ろにずれる量よりも小さいので、全体として重複期間40は短くなる。

【0194】4. 他のシステムにおける実施形態  
上記実施形態では、衛星放送システムに適用した場合について説明した。しかしながら、暗号鍵を用いて行う地上波放送や有線放送についても同じように適用することができる。

【0195】また、ローカルエリアネットワーク（LAN）、ワイドエリアネットワーク（WAN）等において、データを暗号化して通信する場合にも適用することができる。送信側と受信側が1対1の場合にも適用できるが、送信側から複数の受信側に一斉通信する場合に適用するとより好ましい。

【図面の簡単な説明】

【図1】この発明の一実施形態による通信システムの全体構成を示す図である。

【図2】この発明の一実施形態による通信システムにおける暗号化データと鍵対応データの送出タイミングを示す図である。

【図3】本発明を衛星放送システムに適用した一実施形態による送信装置の構成を示す図である。

【図4】送信装置によるデータのバケット化を示すための図である。

【図5】パケット化されたデータの構造を示す図である。

【図6】制御データPATの一例を示す図である。

【図7】制御データPMTの一例を示す図である。

【図8】ECMデータの構造を示す図である。

【図9】制御データNITの一例を示す図である。

【図10】ESデータとECMデータの送出タイミングを示す図である。

【図11】図10の重複期間40近傍の詳細を示す図である。

【図12】本発明を衛星放送システムに適用した一実施形態による受信装置の構成を示す図である。

【図13】デ・スクランブラ68のDSレジスタの記憶内容例を示す図である。

【図14】ICカード80の構成を示す図である。

【図15】ICカード80における鍵復元処理のタイミングを示す図である。

【図16】受信装置のメモリ74に記録された受信処理のためのプログラムを示すフローチャートである。

【図17】図16のステップS6の処理の詳細を示すフローチャートである。

【図18】チャンネル切換が行われた場合の処理を説明するための図である。

【図19】重複期間40の直前にてチャンネル切換が行われた場合の処理を説明するための図である。

【図20】重複期間40内にてチャンネル切換が行われた場合の処理を説明するための図である。

【図21】重複期間40内にてチャンネル切換が行われた場合の処理を説明するための図である。

【図22】重複期間40終了後、鍵変更時点Txまでの間に、チャンネル切換が行われた場合の処理を説明するための図である。

【図23】2つの鍵復元を並行して行う場合における、図16のステップS6の処理の詳細を示すフローチャートである。

【図24】2つの鍵復元を並行して行う場合における、図16のステップS6の処理の詳細を示すフローチャートである。

【図25】チャンネル切換が行われた場合の処理を説明す

るための図である。

【図26】重複期間40の直前にてチャンネル切換が行われた場合の処理を説明するための図である。

【図27】重複期間40内にてチャンネル切換が行われた場合の処理を説明するための図である。

【図28】重複期間40終了後、鍵変更時点Txまでの間に、チャンネル切換が行われた場合の処理を説明するための図である。

【図29】他の実施形態における、ESデータとECMデータの送出タイミングを示す図である。

【図30】他の実施形態における、ECMデータの構造を示す図である。

【図31】図30の重複期間近傍の詳細を示す図である。

【図32】他の実施形態における、図16のステップS6の処理の詳細を示すフローチャートである。

【図33】他の実施形態における鍵再生装置（鍵取得手段）の全体構成を示す図である。

【図34】ICカードのメモリ98に記録されたプログラムのフローチャートを示す図である。

【図35】チャンネル切換が行われた場合の処理を説明するための図である。

【図36】この実施形態において、図16のステップS6の詳細を示すフローチャートである。

【図37】従来の受信機の構成を示す図である。

【図38】従来の鍵の通信方法を示す図である。

【図39】従来の鍵の通信方法を示す図である。

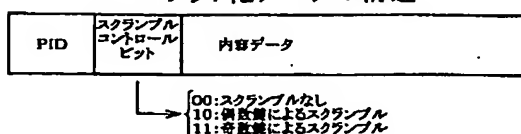
【図40】従来の通信方法における問題点を示す図である。

【符号の説明】

20・・・送信装置  
22・・・鍵出力手段  
24・・・暗号化手段  
26・・・鍵対応データ生成手段  
28・・・送出手段  
30・・・受信装置  
32・・・受取手段  
34・・・復号化手段  
36・・・鍵取得手段

【図5】

#### パケット化データの構造

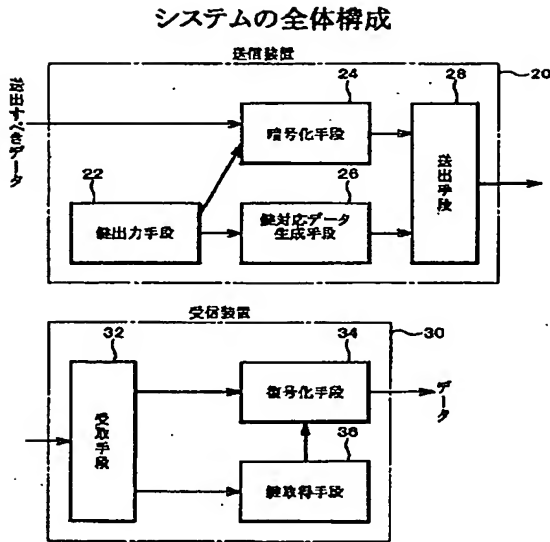


【図6】

#### PAT

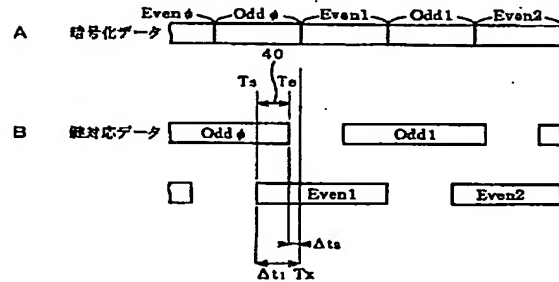
チャンネルNO.	PMTのPID
3ch	●×10
6ch	●×11
7ch	●×12

【図1】



【図2】

暗号化データと鍵対応データの送出タイミング



【図7】

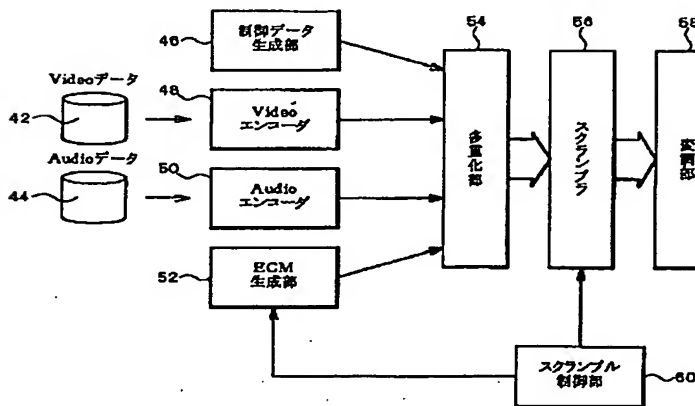
PMT

ビデオ		オーディオ	
ECMのPID	ESのPID	ECMのPID	ESのPID
φ×21	φ×22	φ×21	φ×24

【図3】

【図13】

送信装置の構成



デ・スクランブラのDSレジスタ

PID	Even鍵	Odd鍵
0×8T	101...1	110...1
0×75	—	010...1

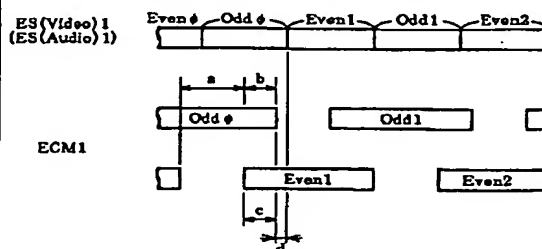
【図9】

【図10】

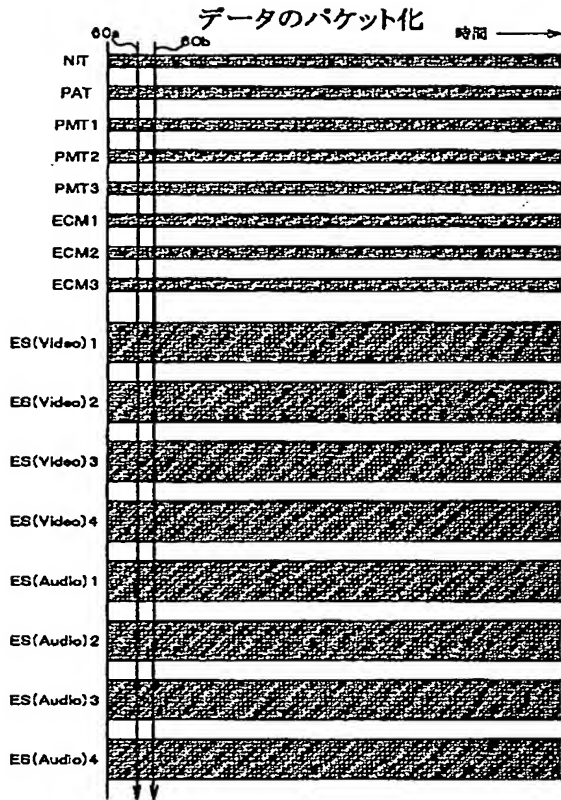
NIT

Ta_id	伝送経路	チャンネルリスト
0	11.2GHz、水平偏波...	0, 1, 2
1	11.23GHz、水平偏波...	3, 5, 7, 9

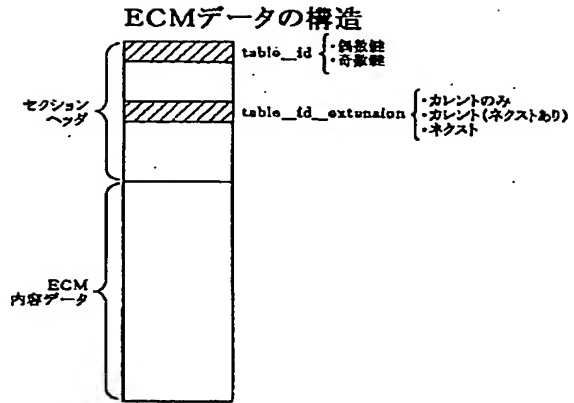
ESデータとECMデータの送出タイミング



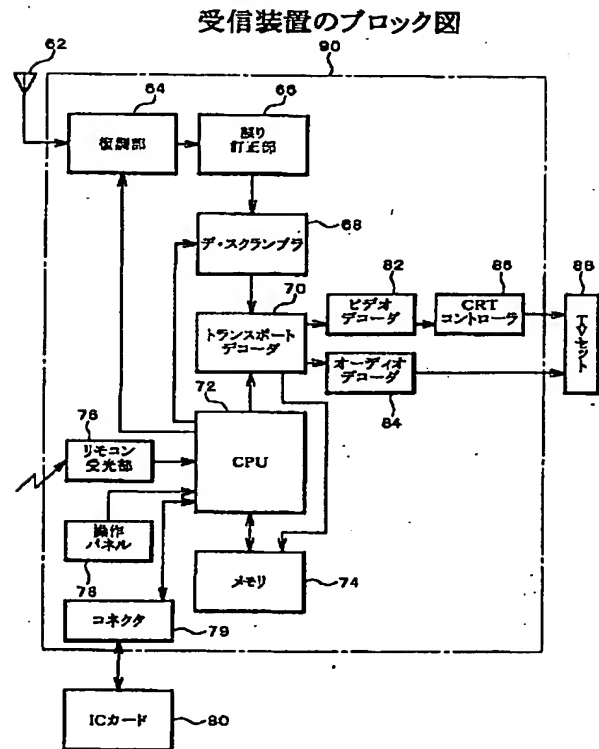
【図 4】



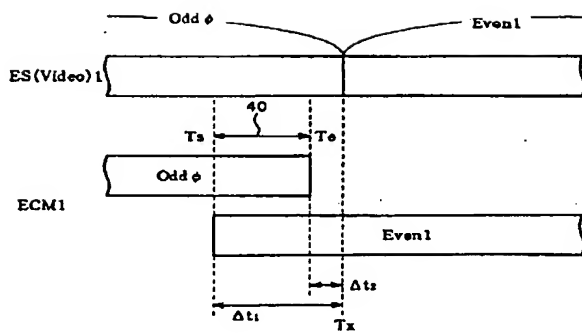
【図 8】



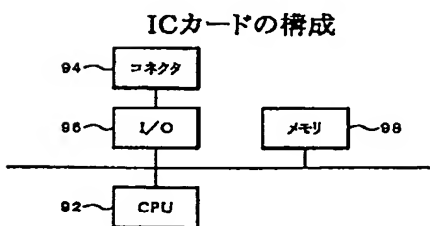
【図 12】



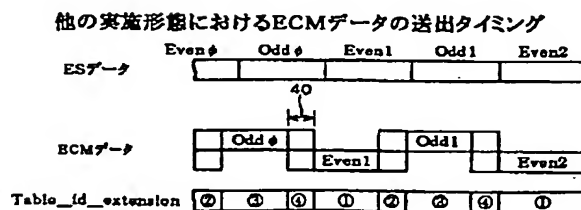
【図 11】



【図 14】

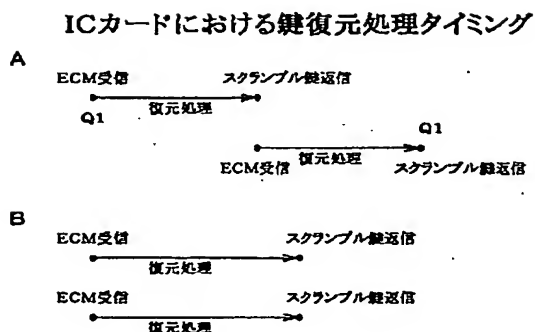


【図 29】

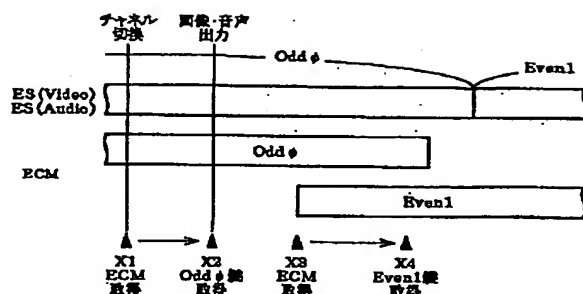




【図15】

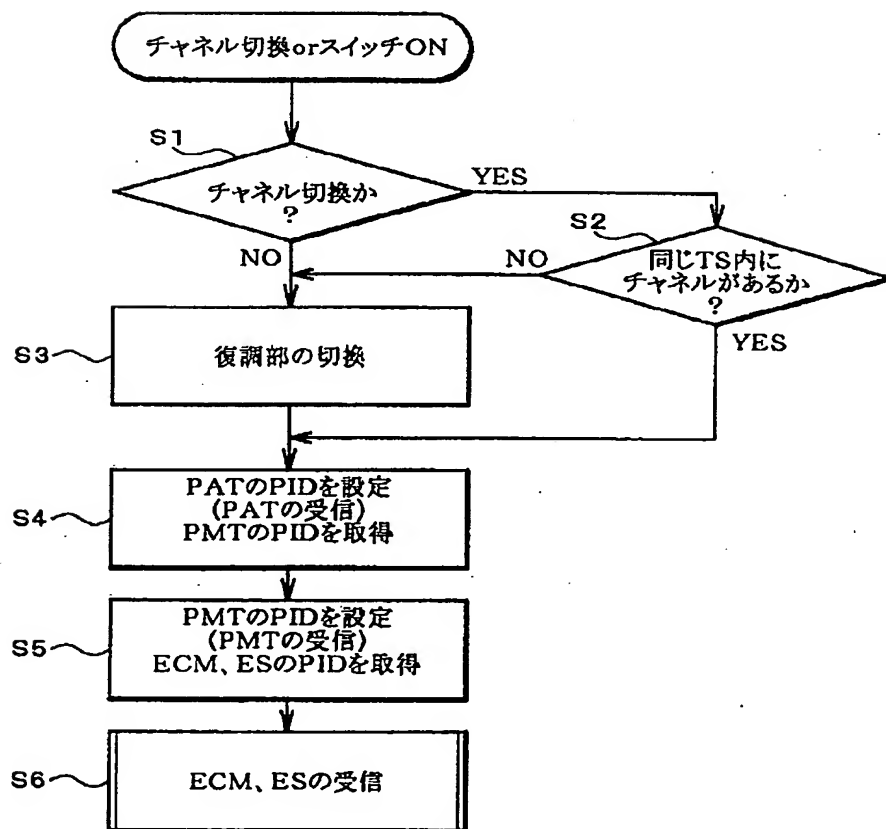


【図18】



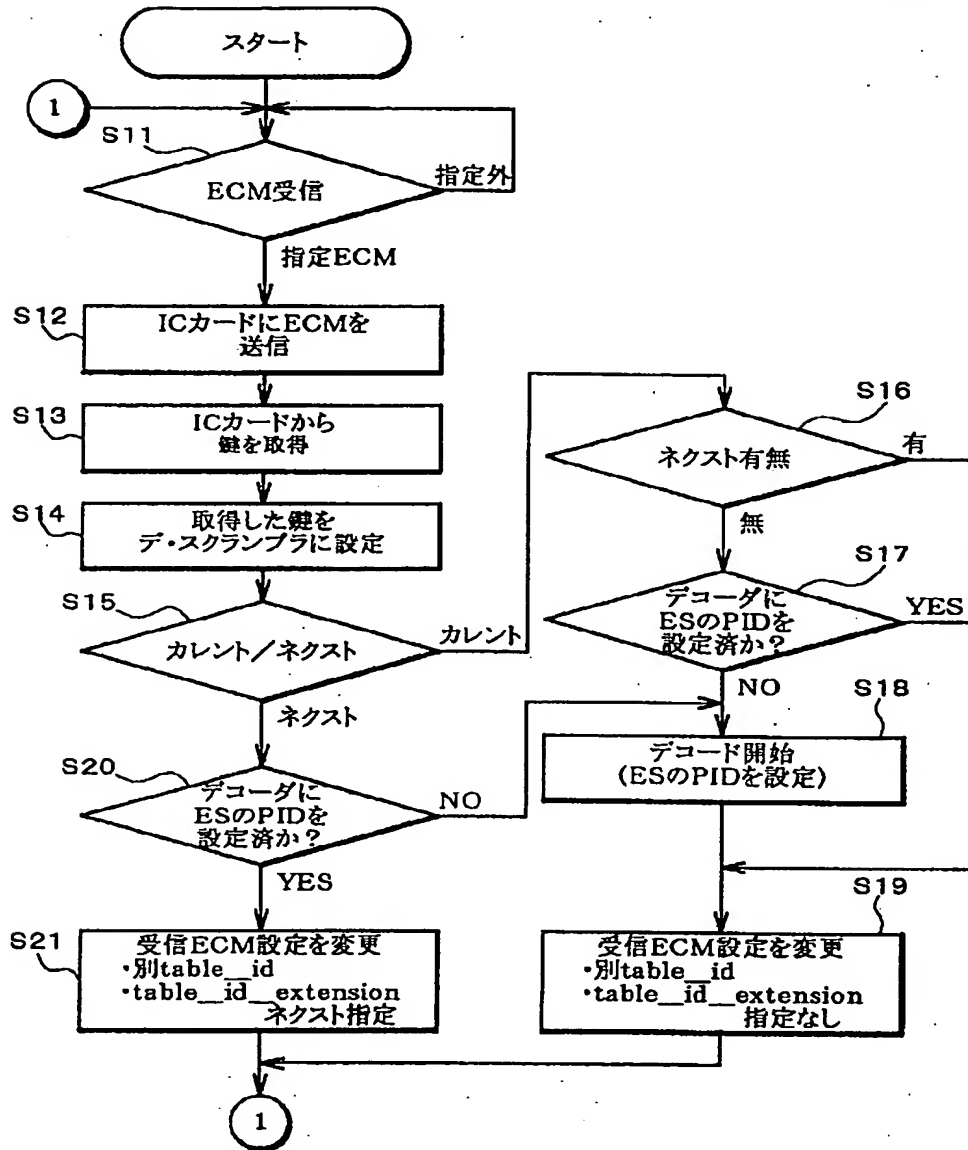
【図16】

# 受信フローチャート

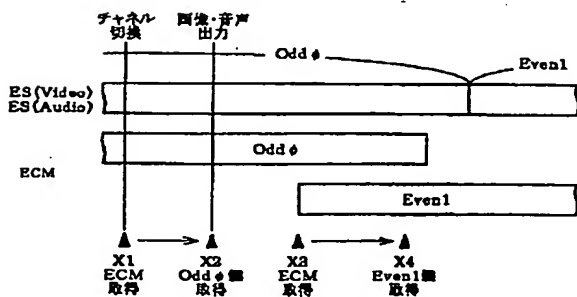


【図17】

ECM、ESの受信処理(詳細) - 鍵復元を1つつ行う場合 -

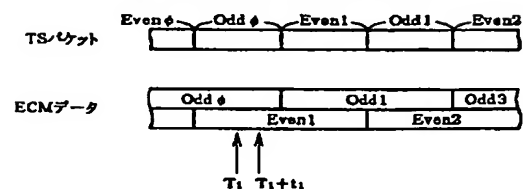


【図25】

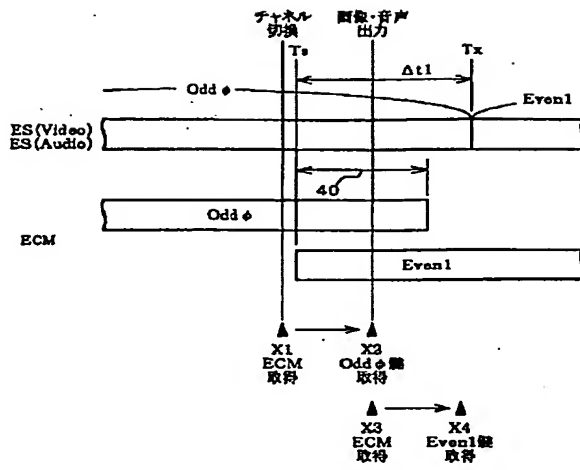


【図38】

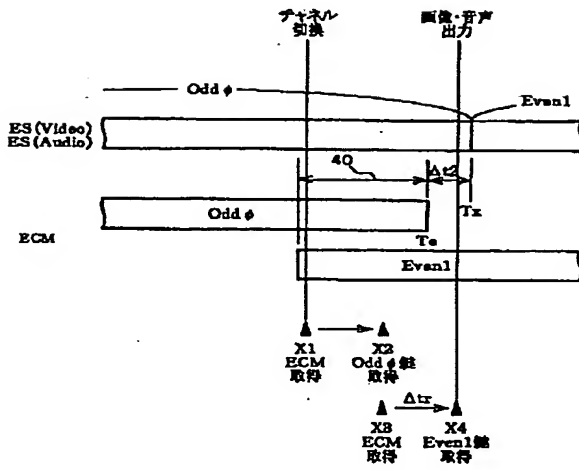
鍵の通信方法(従来技術)



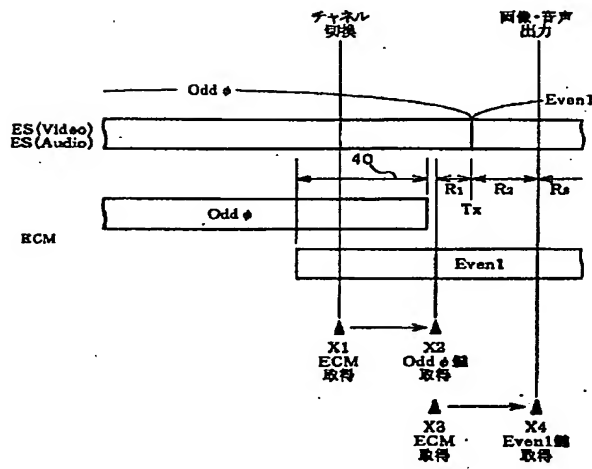
【図 19】



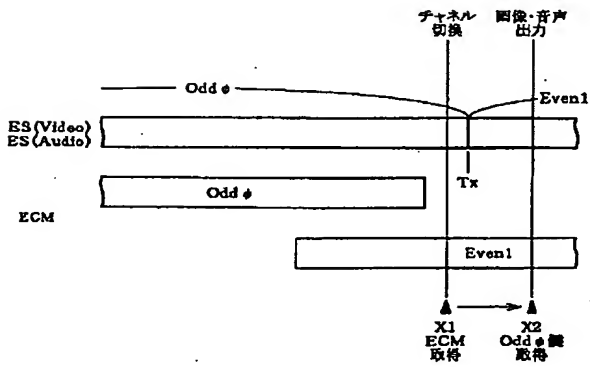
【図 20】



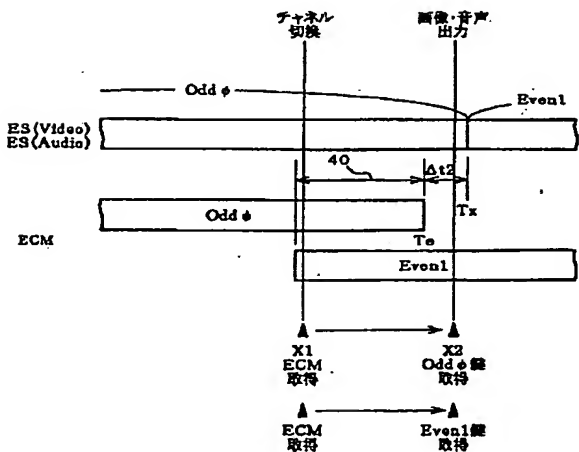
【図 21】



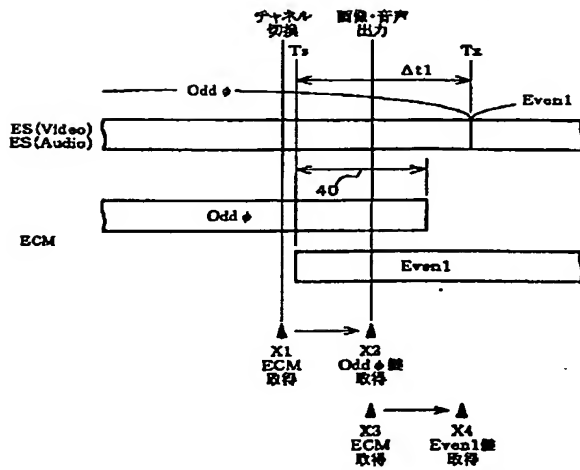
【図 22】



【図 27】

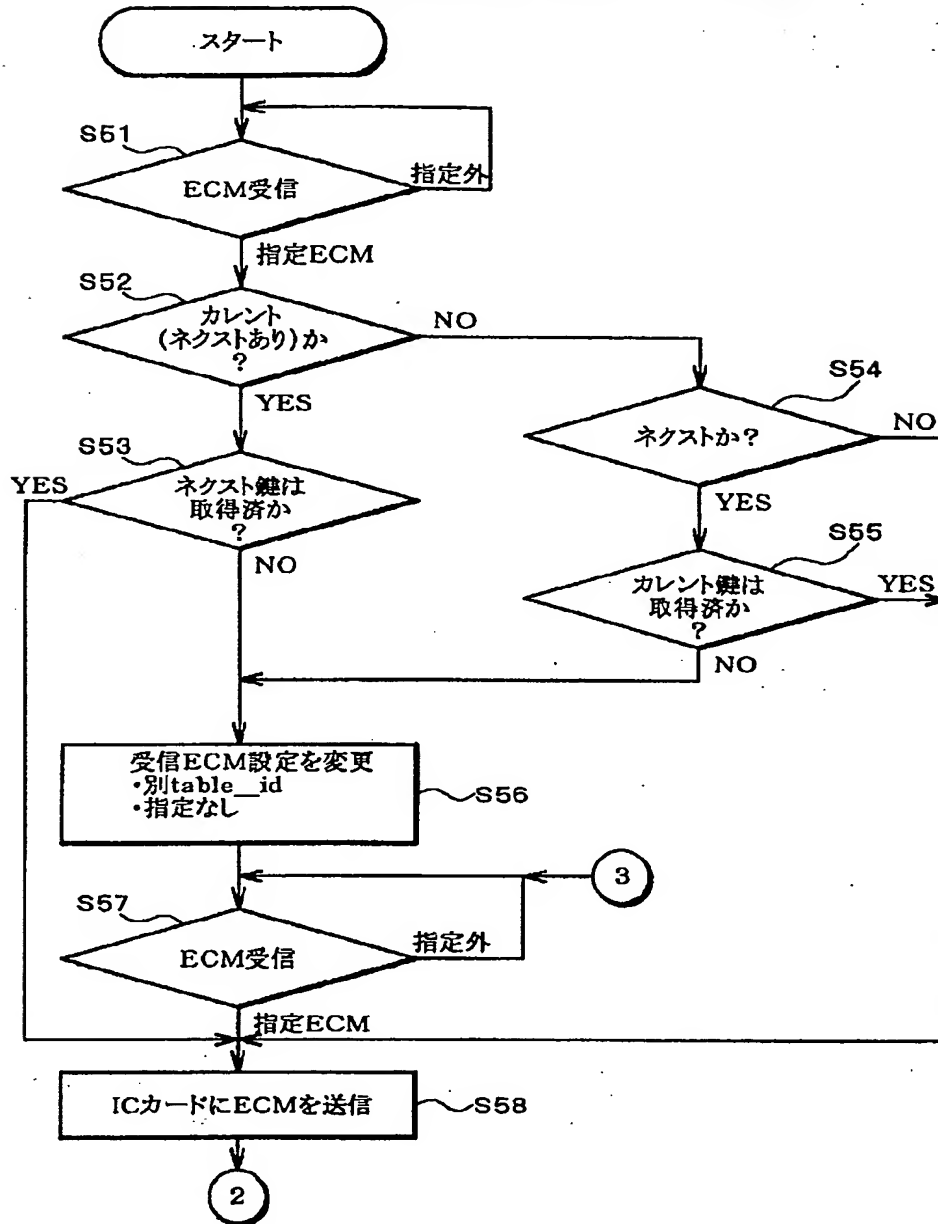


【図 26】



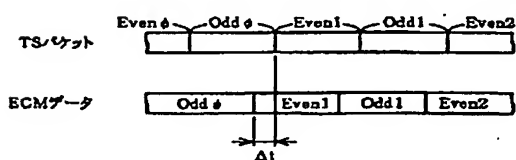
【図23】

ECM、ESの受信処理(詳細)  
-2つの鍵復元を同時に並行して行う場合-

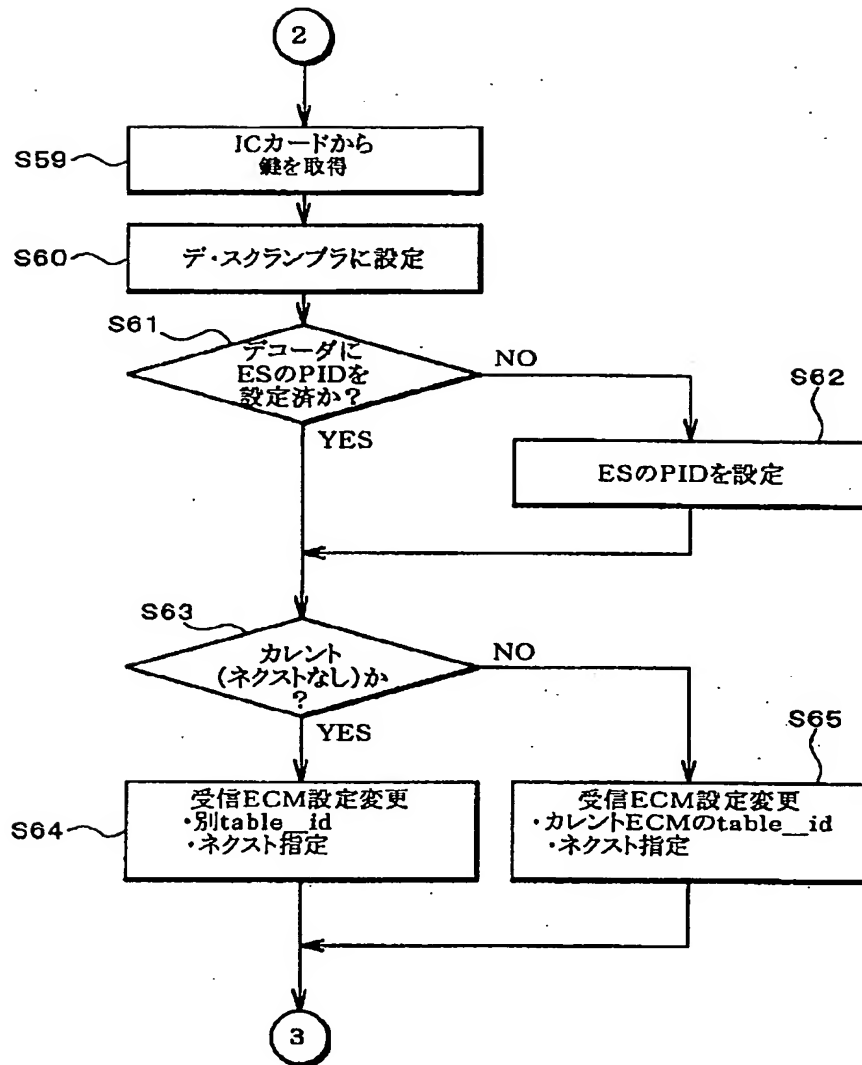


【図39】

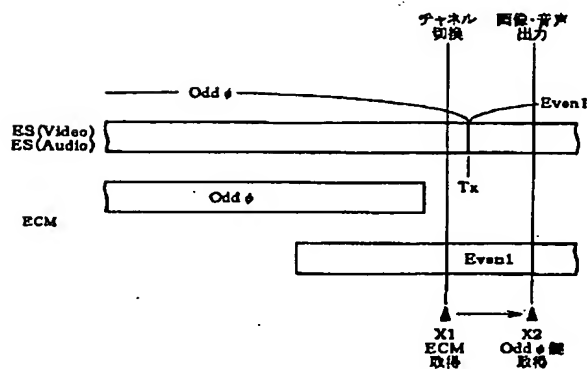
鍵の通信方法(従来技術)



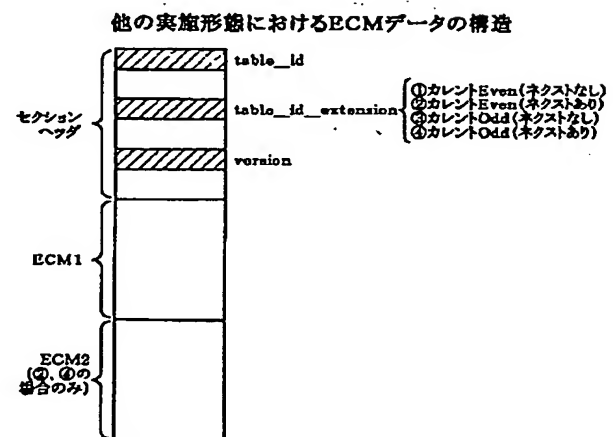
【図24】



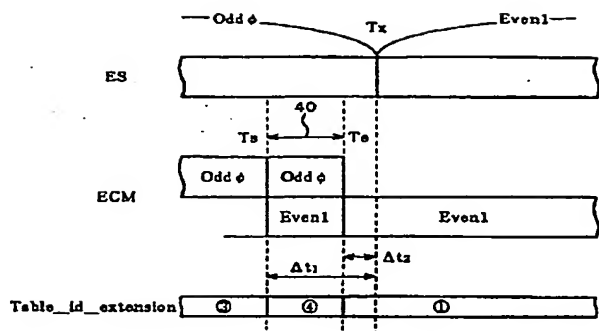
【図28】



【図30】

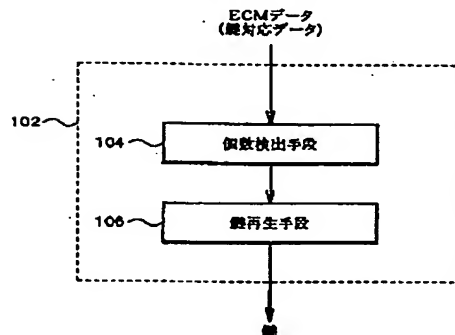


【図31】



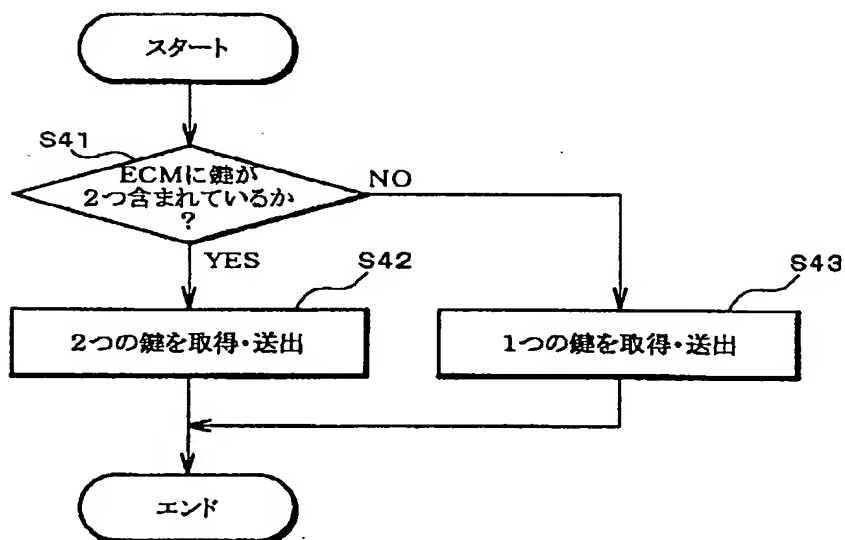
【図33】

鍵再生装置(鍵取得手段)の全体構成

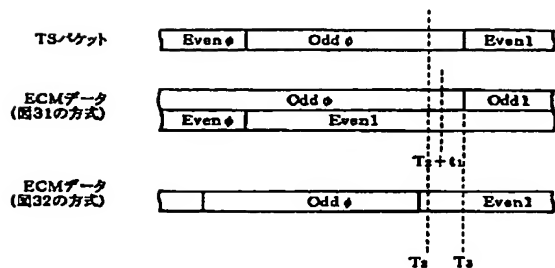


【図34】

ICカードの処理フローチャート

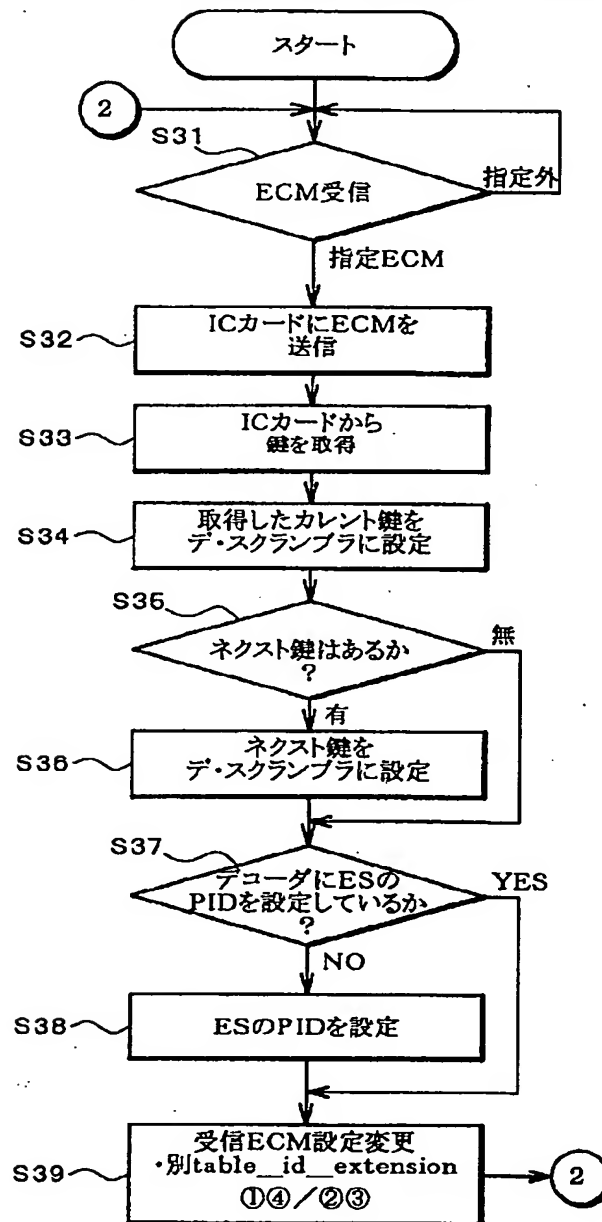


【図40】



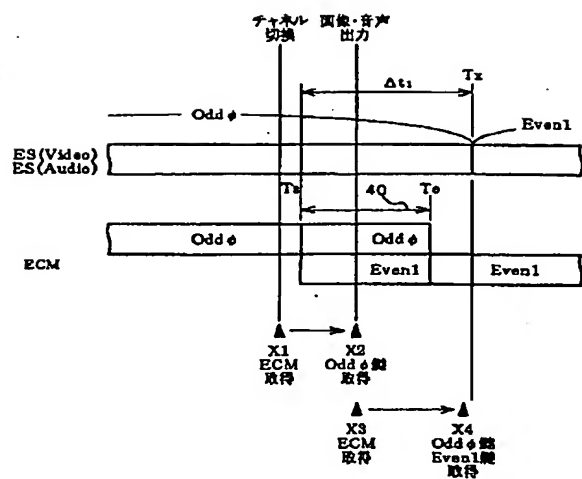
【図32】

## ECM、ESの受信処理(詳細)



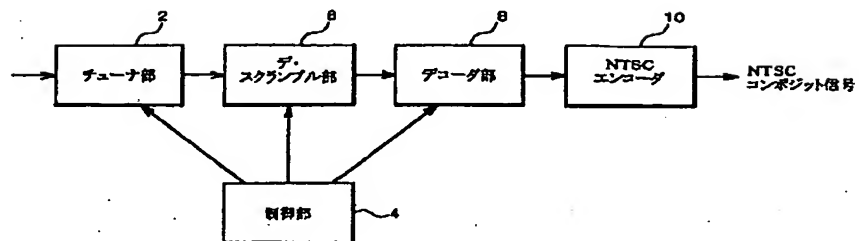


【図35】



【図37】

受信機の構成〈従来技術〉



【図36】

## ECM、ESの受信処理(詳細)

